REGULATION OF E-COMMERCE IN INDIA WITH SPECIAL REFERENCE TO ELECTRONIC CONTRACT

THESIS

SUBMITTED FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

IN

LAW

By

AZMAT ALI

Under the supervision of

Professor IQBAL ALI KHAN
Dean and Chairman, Faculty of Law

FACULTY OF LAW
ALIGARH MUSLIM UNIVERSITY
ALIGARH-202002 (U.P.) INDIA

2015

Dedicated

To

My Parents

DEPARTMENT OF LAW
ALIGARH MUSLIM UNIVERSITY
ALIGARH-202002, INDIA

Prof. IQBAL ALI KHAN
Dean and chairman dated.....

CERTIFICATE

This is to certify that **Mr. Azmat Ali**, Research Scholar, Department of Law, A.M.U., Aligarh has completed his Ph.D. thesis entitled ***"REGULATION OF E-COMMERCE IN INDIA WITH SPECIAL REFERENCE TO ELECTRONIC CONTRACT"*** under my supervision. The material incorporated in the thesis has been collected from various sources; he has used and analyzed aforesaid material systematically. The present work is an original contribution to the field of E-Commerce Law in India.

I wish him all success in life

(Prof. IQBAL ALI KHAN)
Supervisor

ACKNOWLEDGEMENTS

First of all I thank to God Almighty Who's Mercy and Graciousness enabled me to carry out the work.

I wish to express my most humble, sincere and profound gratitude to my erudite supervisor, Prof. Iqbal Ali Khan (Dean & Chairman), Faculty of Law, Aligarh Muslim University, Aligarh, for his cognate attitude, academic excellence, skillful guidance and continuous encouragements towards this work, his keen interest and immense help in an indefatigable and perspicacious manner emphatically paved the way for me to complete the study

I would like to express my sincere thanks to Prof. Javaid Talib, Faculty of Law, AMU, Aligarh who showed me the benign guidance to work on this topic of my research work and despite paucity of time was available.

I would also like to thank my respected teachers specially, Prof. Zubair Ahmad Khan, Prof. Zaheeruddin, Prof. Mohd Shakeel Ahmad, Prof. Mohd Ashraf, Prof. M.Z.M. Nomani, Dr. Badar Ahmad, Dr, Shakeel Ahmad, Dr. Mohd Waseem Ali, Dr, S. Iqbal Hadi Rizvi, Dr. Hashmat Ali Khan, Dr. Tabassum chaudhary, Mis. Rabab khan, Mr. Z. Khairoowala, Dr. Fasih Raghib Gauhar, Dr. Sk. Ehteshamuddin Ahmad, Dr. Md. Rahmatullah, Dr. Kaleemullah and Mr. Salil Kumar for the peers of wisdom that they gave me during my Research.

My sincere thanks to whole ministerial and library staff, Faculty of Law, AMU for their cooperation at each and every stage in the completion of the study.

In addition, I am grateful to all my friends and colleagues for giving me their valuable time to make my study life an unforgettable and memorable period in the university.

My heart fills with earnest gratitude to pay the tributes to Bani-e-Darsgah Sir Syed Ahmad Khan. May Allah bestow eternal peace upon them with Maghfirat and Rahmat.

Last but not least, I owe greatest gratitude to my parents, grandparents and family members, for their unwavering love, affection and prayers. Without their love and enormous support, this thesis would not be possible.

Azmat Ali

CONTENTS

ABBREVIATION

ACH	:	The Automated Clearinghouse
ADR	:	The Alternative Dispute Resolution
AEPC	:	The Apparel Export Promotion Council
APEC	:	The Asia Pacific Economic Co-operation
APEDA	:	The Agriculture and Processed Food Export Development Authority
ARPA	:	Advanced Research Projects Agency
ARPANET	:	Advanced Research Projects Agency Network
ASCAP	:	The American Society for Composers, Authors and Publisher
ATM	:	The Automated Teller Machine
B2B	:	The Business-to Business
B2C	:	The Business-to-Consumer
BBS	:	The Electronic Bulletin Board Systems
BMI	:	The Broadcast Music Inc.
C2B	:	The Consumer-to-Business
C2C	:	The consumer-to-consumer
CA	:	The Certifying Authorities
CAT	:	The Cyber Appellate Tribunal
CBDT	:	The Central Board of Direct Taxation
CCA	:	The Controller of Certifying Authorities
ccTLDs	:	The Country Code Top-Level Domains
CD	:	The Compact disc.
CD-ROM	:	The Compact disc. Random Online Memory
CHIPS	:	The Clearing House Interbank Payment Systems
CPS	:	The Certification Policy Statement
CPS	:	The Certification Practice Statement
CRAC	:	The Cyber Regulations Advisory Committee
CRAT	:	The Cyber Regulations Appellate Tribunal

DGFT	:	The Directorate General of Foreign Trade
DNS	:	The Domain Name System
DNSO	:	The Domain Name Supporting Organization
DoD	:	The Department of Defense
EBBS	:	The Electronic Bulletin Board Systems
E-books	:	Electronic Book
E-commerce	:	The Electronic Commerce
EDI	:	The Electronic Data Interchange
EEZ	:	The Exclusive Economic Zone
EFT	:	The Electronic Fund Transfer
EFTPOS	:	The Electronic Funds Transfer Point of Sale System
E-mail	:	The Electronic Mail
ENIAC	:	The Electronic Numerical Integrator & Computer
ERNET	:	The Educational and Research network
Fax	:	The Fascimile
GATS	:	The General Agreement on Trade in Services
HTML	:	The Hyper Text Markup Language
HTTP	:	The Hyper Text Transfer Protocol
IBM	:	The International Business Machines Corporation
ICANN	:	The Internet Corporation for Assigned Names and Numbers
ICS	:	The Industrial Control Systems
ICT	:	The information and communication technology
IM	:	The Instant Message
IP	:	The Internet Protocol
IPRs	:	The Intellectual Property Rights
ISP	:	The Internet Service Provider
IT ACT	:	The Information Technology Act, 2000
LAN	:	The Local Area Network

NCP	:	The Network Control Protocol
OECD	:	The Organisation for Economic Co-operation and Development
OSP	:	The Online Service Provider
PC	:	The Personal Computer
PKI	:	The Public Key Infrastructure
PLCs	:	The Programmable Logic Controllers
POS	:	Point-of-sale
PPT	:	The Performance and Phonograms Treaty
PTTNS	:	The Public Telecommunications Transport Networks and Services
RDF	:	The Resource Description Framework
RPAD	:	The Registered Post Acknowledgement Due
SCCR	:	The WIPO Standing Committee on Copyright and Related Rights
TCP	:	The Transmission Control Programme
TLD	:	The Trade Level Domain Name
TLD	:	The Top Level Domains
TRIPS	:	The Trade related intellectual property rights
TTPs	:	The Trusted Third Parties
U.K.	:	The United kingdom
U.S.	:	The United state
UN	:	The United Nations
UNCITRAL	:	The United Nations Commission on International Trade Law
UNESCAP	:	The United Nations Economic and Social Commission for Asia and the Pacific
URIs	:	The Uniform Resource Identifiers
VSNL	:	The Videsh Sanchar Nigam Ltd.
WAN	:	The Wide Area Network
WAP	:	The Wireless Application Protocol
WCT	:	The WIPO Copyright Treaty
WIPO	:	The World Intellectual Property Organization

WPPT	:	The WIPO Performances and Phonograms Treaty
WTO	:	The World Trade Organization
WWW	:	The World Wide Web

LIST OF CASES

27. *Dhannatal* v. *Kalawatibai,* (2002) 6 SCC 16
28. *Diamond* v. *Diehr,* 450 U.S. 584 (1978)
29. *Digital Equipment Corp.* v. *AltaVista Technology, Inc.,* 960 F.Supp .. 456 (O.Mass 1997)
30. *Donogue* v. *Allied Newspapers,* (1937) 3 ALL.ER 503
31. *Eckhardt Marine GMBH* v. *Sheriff Mahkamah Tinggi Malaya & Ors,* (2001) 3 Cri LJ 864
32. *EDIAS Software International* v. *BASIS International Ltd.,* 947 F. Supp.413 (1996)
33. *Edias Software International, L.L.C.* v. *Basis International Ltd,* 947 F.Supp. 413 (D.Ariz. 1996)
34. *Enterprises, Inc.* v. *Calvin Designer Label,* 985 F. Supp. 1220 (N.D. Cal. 1997)
35. *Entores Ltd.* v. *Miles Far Eastern Corporation,* (1955) 2 QB 326
36. *Enza Hill* v. *Gateway 2000 Inc,* U.S. Court of Appeals for the Seventh Circuit 105 F. 3d 1147 (1997)
37. *Euromarket Designs Inc.* v. *Peters,* (2001) FSR 20
38. Fatima Riswana v. State Rep. by A.C.P., Chennai and Ors., AIR 2005SC 712
39. *Government of Malaysia* v. *Gurcharan Singh,* (1971) 1 MLJ 211
40. *Groff* v. *America Online, Inc.,* 1998 WL 307001 (R. I. Super C t. 1998)
41. *Hakam Singh* v. *Gammon (India) Ltd,* (1971) 1 SCC 286
42. *Hans Muller of Nuremberg* v. *Superintendent Presidency jail, Cal,* AIR 1955 SC 367
43. *Hartford Fire Insurance Co.* v. *California,* 113 S. Ct 2891 (1993)
44. *Hotmail Corporation* v. *Van Money Pie Inc.,* C98-20064 (ND Ca, 20 April 1998)
45. *Carlil* v. *The Carbolic Smoke Ball Company,* (1893) 1 QB 525
46. *Indian Cable Co. Ltd.* v. *CCE,* (1994) 6 SCC 610
47. *Quality Steel Tubes (P) Ltd.* v. *CCE,* (1995) 2 SCC 372
48. *Dr. Prakash* v. *State of Tamil Nadu and Ors.,* AIR2002SC3533
49. *International Shoe Co.* v. *State of Washington, Office of Unemployment Compensation and Placement ei al,* 326 US. 310.316 (1945)
50. *Joyce* v. *Director of Public Prosecutions,* 1946 App Cas . 347
51. *K.K. Velusamy* v. *N. Palanisamy,* MANU/SC/0267/2011
52. *Kepong Prospecting Ltd.* v. *Schmidt,* (1968) 1 MLJ 170

53. *L.M.S. Umma Salemma* v. *B.B. Gujaral*, (1981) 3 SCC .317.
54. *Mahomed Syedol Ariffin* v. *Yeoh Ooi Gark*, (1916) 2 *AC* 575, PC (Penang)
55. *Maritz, Inc.* v. *Cybergold, Inc.*, 947 Fsupp.1328 (E.D.Mo. 1996)
56. *Minnesota* v. *Granite Gate Resorts Inc.* , 569 N.W. 2d 715 (Mn.APP.Ct.1997)
57. *Mohori Bibee* v. *Dhurmodas Ghose*, (1903) 30 Cal 539; 30 1 a114, PC (India)
58. *MP Verma* v. *Surinder Kaur*, AIR 1982 SC 1043
59. *New York* v. *World Interactive Gaming Corp*, No. 404428/98 (Sup. Ct. N.Y. City July 22, 1999)
60. *Phiong Khon* v. *Chonh Chai Fah* (1970) 2 MLJ 114, FC
61. *Planned Parenthood Fed'n of Am.* v. *Bucci*, No. 97 Civ. 0629, 1997 U.S. Dist. LEXIS 3338 (S.D.N.Y. Mar. 19, 1997)
62. *ProCD, Inc* v. *Zeidenburg*, 86 F.3d 1447 (7th Cir. 1996)
63. *PurCo Fleet Services, Inc.* v. *Towers*, 38 F.Supp.2d 1320 (D. Utah 1999)
64. *Rajasthan High Court Advocates' Association* v. *Union of India*, (2001) 2 SCC 294
65. *Rambabu Saxena* v. *State*, AIR 1950 SC 155
66. *Ratan N. Tata* v. *Union of India (UOI) and Ors.*, MANU /SC/1090/2013
67. *Shreya Singhal* v. *Union of India*, Writ Petition (Criminal) No.167 of 2012 held on March 24, 2015.
68. *Smith v. Hobby Lobby Stores Inc.* v. *Boto Co. Ltd.*, 968 F. Supp. 1356 (W.D. Ark. 1997)
69. *Specht* v. *Netscape Communications Corp*, 2000 United States Dist. LEXIS 12897 (C.D. 2000); aff'd 248 F. 2d 1173 (9th Cir. 2001)
70. *Specht* v. *Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001)
71. *SS Lotus Case (France* v. *Turkey)*, PCIJ Ser A (1927), No. 9
72. *State of Delhi* v. *Mohd Afzal & Others*, 2003(3) 11 JCC 1669
73. *State of Minnesota* v. *Granite Gate Resorts, Inc*., Court File No. C6-95-7227
74. *State of Punjab* v. *Amritsar Beverages Ltd. and Ors.*, AIR2006SC2820
75. *State* v. *Navjot Sandhu*, (2005) 11 SCC 600
76. *Step-Saver Data Systems, Inc* v. *Wyse Technology*, 939 F 2d 91 (3rd Cir 1991)
77. *Tata Consultancy Services* v. *State of Andhra Pradesh*, AIR 2005 SC 371
78. *Telco Communications* v. *An Apple a Day*, Civ. Act.No 97-542 (E.D.Va.1997)
79. *Twentieth Century Fox Film* v. *Nri Film Production Associates* , AIR 2003Kant 148

80. United States v. *Romano,* 706 F.2d 370 (2d Cir .1983)

81. United States v. *Thomas,* 74 F.3d 701 (6th Cir. 1996)

82. Washington Post Co. v. *Total News Inc.,* No. 97 Civ. 1190 (PKL)(S.D.N.Y. filed February 20, 1997)

83. Whelan Associates, Inc. v. *Jaslow Dental Laboratory, Inc.,* 797 F.2d 1222 (3d Cir. 1986)

84. *Wong Hon Leong David* v. *Noorazman bin Adnan*, (1995) 3 MLJ 283

85. Woolmillgton v. *Director of Public Prosecutions,*1935 AC 462;SHC 39

86. Zippo Manufacturing Company v. *Zippo Dot Com, inc.,* 952 F. Supp.1119 (W.D.Pa.1997)

LIST OF AUTHOR'S PUBLICATIONS AND PAPER PRESENTATIONS IN CONFERENCES AND WORKSHOPS

Publications

- Azmat Ali, "**Legality of Electronic Contract in Indian Legal Environment**" Vol-1 No-3 International Journal of Society and Humanities, pp.246-252 (2013) ISSN-23192070.
- Paper Presentation on National Conference "**Women's Right to Health and Commercial Surrogacy in India: Legal Issues and Perspective**" Organized by College of Law & Legal Studies Teerthanker Mahaveer University Moradabad held on 2nd May (2015) ISBN 9789352126910.

INTRODUCTION

With the advent of internet and its commercialization since 1994, E-Commerce rapidly emerged in the new world economy. E-commerce may be defined as the use of the internet and other networking technologies for conducting business transactions. Nowadays most people think E-Commerce means online shopping. However, web shopping is only a small part of the picture. In addition, E-Commerce includes business-to-business connections that make purchasing easier for big corporations. Furthermore, E-Commerce will significantly have impact the global economy as well as play a vital part in future economic development. Several developing countries have started to pursue policies to provide a consistent legal and regulatory framework to support electronic transactions across state, national and international borders.

The growth of E-Commerce has required the vibrant and effective regulatory mechanism to further strengthen the legal infrastructure to the success of E-Commerce in India. But, all these regulatory mechanisms as well as legal infrastructure come within domain of cyber law. However, nowadays awareness about cyber law has begun to grow. Initially, several technical experts considered that legal regulation of the internet was not necessary, but fast growth of technologies and the internet compelled to think that no activity on the internet could have remained free from the influence of the cyber law because feature of the internet, which caused much controversy in the legal community.

The World Trade Organization (WTO) Ministerial Declaration on E-Commerce defines E-Commerce as the production, distribution, marketing, sales or delivery of goods and services by electronic means. According to European Commission, E-Commerce encompasses more than the purchase of goods online. It includes a disparate set of loosely defined behaviours, such as shopping, browsing the internet for goods and services, gathering information about items to purchase and completing the transaction. It also involves the fulfilment and delivery of those goods and services and inquiries about the status of orders.[1] That is, E-Commerce is all about commercial transactions, whether between private individuals or

[1] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.780 (Kamal Law House, Kolkata, 1st ed., 2008).

commercial entities, which take place in or over electronic networks. The only important factor is that the commercial transactions take place over an electronic medium. It can be conducted over Telephones, Fax Machines, Automatic Teller Machines (ATMs), and electronic payment systems such as prepaid telephone cards, electronic data interchange (EDI), television and the internet.

With the advent of technology, intellectual property laws over the years have undergone changes. But, challenges imposed by the development and growth of internet are immense especially to copyright. A key question whether jurisdiction should be determined by reference to where material originated, where it went along the way or where it ended up being displayed, stored or printed out. It may be correct to say that an infringement has taken place and under more than one law. Another problem is of choice of law as jurisdiction may arise in number of countries. The law of each country is different. For e.g. under Indian Law compulsory registration of work is not required where as in United State copyright law requires compulsory registration. Uniformity of law is requirement of E-Commerce.

The issues related to Electronic Data Interchange and particularly the internet have opened up not only vast possibilities for electronic commerce but also posed various problems for the taxman. Taxation issues relating to electronic commerce are not confined to customs duties alone. Equally important concerns arise in relation to domestic taxes such as sales tax, value added tax and income tax relating to sale of products over the internet. It is no small challenge to experts in taxation, law and economics to design an equitable tax system for electronic commerce.[2] Moreover, the United State proposal to the World Trade Organisation (WTO) does not answer the problematic issues relating to customs duties on electronic commerce but merely avoids them by proposing zero duty. It is not known if all World Trade Organisation (WTO) members will accept the United State proposal. Even if they do similar, problems in other areas of taxation would still remain unless zero tax treatment is extended to all electronic commerce. No doubt, exemption from customs, sales tax, VAT (Value Added Tax) and income tax will give a tremendous boost to electronic commerce.

---

[2] C Satapathy, "Taxing Electronic Commerce" *Economic and Political Weekly* p.1068 (May 9, 1998).

However, it has become essential to create a policy and regulatory environment that favours the development of E-Commerce and harmonises national approaches in diverse areas such as telecommunications, trade, competition, intellectual property, privacy, and security. Consequently, a series of legal issues need to be effectively addressed before E-Commerce can be considered a safe and effective way of conducting business. Key legal issues arising out of E-Commerce transactions include protection for authentication and no repudiation. This means that there should be a manner of authenticating the identity of the person entering into the transaction. Furthermore, there should be some protection that the person entering the transaction cannot repudiate the same at a later stage. E-Commerce has also given rise to a new breed of crimes called cyber crimes. There is a strong need for cyber policing to reduce the internet's abuse for carrying out crimes that are, at times, more harmful than physical destruction.

The World Wide Web (WWW) has brought new opportunities and challenges to various people. The businesses utilize it for their benefit by expending their activities not only in physical space but also in virtual space in search of the potential customers. Thus, contracting becomes a fundamental element in E-Commerce world. The electronic contracting raises various new legal issues. The nature of the internet is global medium of communication comprising a global web of linked networks and computers has created issues for the formation of common contracts which create complex jurisdictional problems, ignited debate on privacy and defamation issues, created new intellectual property rights which require protection and created a variety of complex consumer protection issues which may not be covered by present legislation.

The internet has transformed the manner of conducting commercial transactions and has created regulatory gaps. These regulatory gaps may impact the effective development of electronic commerce. Attempts are being made to regulate electronic contracts both at the national and international level.[3] Business conducted through the internet caters to globally located customers. This raises cross-border legal issues. Transactions that may be legal and valid in one jurisdiction may not be enforceable in others. Issues relating to the conclusion and enforcement of contracts

[3] F. Tasneem, "The Legal Issues of Electronic Contracts in Australia" 1(2) *International Journal Management Business Research* pp.85-92 (2011).

and choice of appropriate jurisdiction create interpretational issues. It is ultimately left to a court's discretion to decide whether it can try a particular matter brought before it. There are certain theories, such as "*the minimum contact theory*," that has been applied by several courts across the world to determine whether the particular court has jurisdiction to try a particular case. However, there are no defined principles for application of these theories yet. Therefore, there is a need for a uniform act governing transactions that are conducted over the internet.

To provide security and legal recognition to the transactions executed electronically, Indian Parliament enacted the Information Technology Act, 2000 which has come into force on October 17, 2000. This Act, although, modelled on UNCITRAL's Model Law, departs in many respects from the spirit of the Model Law. Furthermore, the Indian courts have not yet found any opportunity to appraise the impact of the provisions of The Information Technology Act, 2000 on substantive principles of contract formation codified in the Indian Contract Act, 1872. An analytical evaluation is, therefore, needed to identify the issues raised by the information technology relating to contract formation and impact of The Information Technology Act, 2000 on the principles relating to contract formation provided in the Contract Act and impact of non inclusion of the principles governing E-Commerce, provided in the Model Law but not reflected in The Information Technology Act, 2000 and the jurisdictional issues which are not confined to national boundaries but have global ramifications and are bound to arise in E-Commerce disputes. [4] Immediately after the enactment of The Information Technology Act, 2000, it was found that certain significant provisions were missing in this enactment and its provisions lacked harmony, and above all many legal issues had not been properly spelled out. This Act was amended in the year 2008 with many objectives. An attempt is made to analyze the legal provisions relating to E-Commerce in The Information Technology Act, 2000, together with the provisions of the Indian Contract Act (Contract Act), which continues to be the fundamental law on the subject.

The Information Technology Act, 2000 is the legal framework governing E-Commerce activities in India. The Information Technology Act, 2000 stipulates

[4] Farooq Ahmad, "Electronic Commerce: An Indian Perspective" 9(2) *International Journal of Law and Information Technology* pp.133 (2001).

various administrative and procedural guidelines for all electronic or computer data related transactions, including electronic document authentication by way of electronic signatures, data protection or deterring heinous crimes like child pornography. The Controller of Certifying Authorities (CCA) is the notified authority for ensuring effective implementation of the Act. The Controller of Certifying Authorities discharges the role of regulating both E-Governance as well as E-Commerce. The Information Technology Act, 2000 clearly excludes transactions through negotiable instruments (other than a cheque) or power of attorney from the scope of its applicability. The Information Technology Act, 2000 also does not enable the creation of a trust, execution of a will and the execution of any contract of sale or conveyance of immovable property or any interest in such property electronically. Owing to its limited scope, The Information Technology Act, 2000 has failed to provide a proper locus for electronic execution of private contracts. However, the most important limitation to the scope of The Information Technology Act, 2000 is that the Act governs execution of only such electronic documents that have been mandated by any other applicable Indian law to be executed in a prescribed manner. Since, the Indian Contract Act, 1872 does not mandate contracts to be executed in writing and the parties to the contract have the liberty to negotiate the format of their contract, The Information Technology Act, 2000 does not throw any light on this aspect of E-Commerce.

The Information Technology Act, 2000 also applies to an offence committed outside India by any person, irrespective of his nationality, so long as the computer system is located in India. Thus, mere presence of the computer system in India is sufficient for an offence to be committed in India. Further, while the Information Technology Act, 2000 is the first step toward recognition of the need to protect and regulate E-Commerce, it suffers from several lacunas in it. One such lacuna is that the act is technology dependent, meaning it only recognises public key infrastructure as a form of digital signature, (now amended by the Amendment Act, 2008 inserted a word electronic signature) when other methods of authentication and identification (such as biometrics) are already developing across the world. Ideally, The Information Technology Act, 2000 should have been technologically neutral, so that it could address all forms of technological advancements. Further, The Information Technology Act, 2000 provides for definitions of certain terms that are ambiguous,

while others include terms, which may lead to interpretational issues. The Information Technology Act, 2000 also contains certain clauses that are contradictory to one another.

All sovereign independent countries possess jurisdiction over all persons and things within its territorial limits and all cases; civil and criminal, arising within these limits. The internet impacts in major ways upon questions of jurisdiction. Jurisdiction to prescribe laws and adjudicate disputes historically has been based on territorial principles, if a country found a person within its territory, it exercised jurisdiction over that person. The internet greatly diminishes the significance of physical location of the parties, because transactions in cyberspace are not geographically based. Moreover, the internet alters the power balance between distributor and consumer because it gives consumers instant access to enormous amounts of information and highly sophisticated analytical tools. This affects the basis on which courts have analyzed the ability of parties and particularly consumers to make enforceable choices of law.

However, the problem would arise when their customers are from different countries and they are transacting with them through their website. This dispute resolution mechanism, based primarily on territoriality, faces a number of challenges when applied to disputes arising on the internet. The Internet is by definition international and can be accessed from almost any place on Earth hence multi-jurisdictional. On the internet, digitized data may travel through various countries and different jurisdictions in order to reach its destination. For example, a dispute may arise between two parties who entered into contract on the internet and who belong to different countries. This is the problem to determine the courts of which country should have jurisdiction to determine this dispute and the laws of which country should be relied upon to determine the dispute. These are the questions which creates problems while deciding jurisdiction in dispute resolution. As a result, the laws relating to simple concepts such as formation, performance and payment under the contract, or even jurisdiction over criminal acts, do not answer to the standard tests laid down in this regard over the past few centuries.[5]

[5] Rahul Malthan, *The Law Relating to Computers and The Internet* p.156 (Butterworths, India 1st edn., 2000).

Thus, E-Commerce includes several issues relating to organizational management, commercial negotiations and contract, legal and regulatory frameworks, financial settlement arrangements and taxation, among many others. Internet facilitates online execution of commercial transaction. It may be either business to business or business to consumer or inter-organizational. The growth and development in the field of E-Commerce has equally needed an effective regulatory mechanism. Cyber law is still a constantly evolving process. With the growth of internet, some issues are also growing relating to jurisdiction, cyber crime, admissibility of e-transaction. Electronic Commerce (EC)/Electronic Data Interchange (EDI)is revolutionizing the way people look at commercial as well as administrative exchanges of information because it does not require paper. In the world of paper documents, the established norms of contract and commercial law have been sufficient to resolve legal disputes concerning these documents. However, an EDI imposes new risks and behaviour related to legality electronic data interchange transaction, digital signature, and the risk of erroneous transmission, lost record, sabotage and fraud.

Thus, the legal issues of Electronic Commerce are related to the evidential, contractual and liability. The law of contract being the area of private law and the brainchild of corporate world the underlying postulate in any legal regime governing contractual relations, that the contracting parties must get freedom to contract, adhere to contract terms and conditions of and also get adequate redress in the event of breach thereof. The basic issues involved any contract are; acceptance; communication; consideration; competency of parties and remedies for breach of contract. In recognition of the increasing number of international transactions executed by means of electronic commerce. International law on electronic contracts appears to have resolved the doubts previously applicable to “shrink wrap” and “click-wrap” contracts.

Difficulty may arise in determining the appropriate jurisdiction of the execution and performance of contract that has been entered into electronically. The legal issues and problems arising from E-Contract have not so for been properly addressed or adjudicated by our courts in India and so the skepticism of the contacting parties regarding the legal principles to be applied is not well founded despite the fact that the Information Technology (Amendment Act 2008) Act, 2000

the allied amendments to the Indian Penal Code, 1860, The Indian Evidence Act, 1872, is a timely legislative attempt to tackle some of the complicated legal issues and problems. The Information Technology Act, 2000 is supplemental to the existing provisions of Indian Contract Act, 1872. Hence, it is a critical appraisal of the existing legal regulation governing of E-Commerce in India with special reference to Electronic Contract.

1. The Choice of Topic

The present study guides the choice of the researcher in the following way:

1. The advent of information technology and its applications have the impact on human beings regarding to E-Commerce, E-Contract, cyber jurisdiction and electronic signature.
2. The E-Commerce on cyberspace has to be regulated and controlled by effective and dynamic legal mechanisms in present legal system.
3. Indian legal system seems to have failed to control the growing menace of cyber commercial based criminality.
4. An adequate legal mechanism is required to control the system with efficient and effective legal regulatory framework.

2. Need for the study

The need for the present research originates from burning issue relating to regulation of E-Commerce in India in contemporary development of modern versions of science and technology. This study is an attempt to fulfil present need and to provide some valuable contributions to develop the technology based effective legal system for the benefit of modern civilized society in order to attain the global perspectives of legal developments. The concern of effective legal regulatory mechanism to regulate E-Commerce in India has urgent need for research in this challenging area.

3. Objectives of Study

The objectives of this thesis are as follows:

1. To find out the historical aspect of E-Commerce in India.

2. To identify the changes in regulation of E-Commerce brought by The Information Technology Act, 2000 based on model law of UNCITRAL on E-Commerce.
3. To analyse the status of present law relating to the admissibility of electronic transaction, cyber commercial crimes and jurisdiction on internet.
4. To focus how cyber law help in flourishing the E-Commerce and how the payment mechanism, encryption, digital signature and computer evidence, help in smooth functioning of E-Commerce.
5. To evaluate the impact of The Information Technology Act, 2000 on the principles relating to contract formation provided in the Indian Contract Act, 1872 and impact of non inclusion of the principles governing E-Commerce.
6. To evaluate the position of protection of Intellectual Property Right specially the software copy right and domain name.
7. To examine the role of The Information Technology Act, 2000, to ensure protection of E-Commerce and prevention of Cyber Commercial Crime.
8. To evaluate whether traditional (paper based) commercial contract principles and digital commercial contract can go together.
9. To study the National and International efforts taken to regulate the E-Commerce.

4. Research Hypothesis

The present research proceeds on the following hypothesis:

3. The development of Information Technology imposes new legal challenges, which requires new legal mode of thinking and behaviour because the existing legal mechanism is not sufficient to deal with all legal issues concerning E-Commerce and E-Contract.
4. The present Information Technology Act, 2000 is not potent enough to protect interest of the E-Consumer, Intellectual Property Right and Protection of Domain Name.
5. In the offline world of paper based documents, the established norms of contract and commercial law have been almost sufficient to resolve disputes

concerning these documents. So far as the digital world on internet is concerned, E-Commerce has posed serious legal risks and problems relating to digital form of document on existing legal system which has failed to resolve all issues concerning E-commerce.

6. The provisions of the Information Technology Act, 2000 and Indian Contract Act, 1872 are not so explicit to resolve the complex issue relating to formation of E-Contract in India.
7. The existing doctrine relating to E-Commerce has become irrelevant due to the unlimited extent with constant development of science and technology. Therefore, the adequate legal regime or reinterpretation of the existing doctrine has to be made to resolve existing legal problem.

5. Scope and limitation of the study

The scope of present study is restricted to the following:

1. The concept of E-Commerce, E-Contract under digital technology and jurisdictional aspect of E-Commerce in cyberspace.
2. Technological development and regulation of E-Commerce under effective legal framework.
3. An adequate legal framework and control mechanisms of regulation of E-Commerce in India.
4. Unlimited possibilities of internet and restricted use of data message in the formation of E-Contract by application of data protective laws.
5. The steps taken by United Nations through the conventions to resolve the problem.
6. The International regulations pertaining to E-Commerce and E-Contract in several countries along with judicial response, conventions at International level and Indian perspective.
7. Legal limitations, difficulties and possible remedial measures.

6. Impact of the study

The technology has always been the boon or bane to human civilization. The subject matter of the present study is so delicate that it has its own inherent

controversies and concerns. However, the impact of the present study would certainly be helpful to add and to develop the existing legal regulatory framework on the subject. Furthermore, with the advent of information technology and internet would not have had the impact that it had as so such brain power has involved into creating the problem of misuse of the internet.

7. Research methodology

The proposed research study is doctrinal and analytical. It is based on critical, descriptive and analytical study of various legislations of different countries, international and regional conventions and Indian legal framework relating to E-Commerce. The proposed study has been carried out in a very objective, systematic and unbiased manner. All the primary and secondary documentary sources have been utilized to make the study advanced, orderly and methodical. Various reports, articles, judicial decisions, international, national, constitutional norms and national measure have been taken as important research tools. Doctrinal method comes in handy for elucidating the international legal framework of E-Commerce and in describing the current state of legal application of E-Commerce and benefit sharing laws adopted by the countries in question in their domestic jurisdiction issue on cyber space. This analysis involves a review of the relevant international treaties, national legislation, policy guidelines, and jurisprudence. It encompasses legal and institutional issues related to E-Commerce in national and international contexts, and a normative consideration of E-Commerce regulation policy in general. The study will certainly enrich the existing knowledge E-Commerce in India.

8. Literature review

The present study will require in-depth study of regulation of E-Commerce laws in selected jurisdictions. Study also requires various international and national legal instruments such as United Nation Convention on International Trade Law, European Electronic Commerce Directive, Uniform Electronic Transaction Act, World Intellectual Property Organization, World Trade Organization, and Indian Legislation: Information Technology Act, 2000. The researcher had gone through several important literatures regarding the topic in form of the Books, Journals, Articles, and Websites etc. The following literature review encompasses works pertaining to Regulation of E-Commerce in India with special reference electronic

contract. Works are pulled from peer-reviewed journals as well as grey literature being produced by NGOs (Non-Governmental Organisation) in the field. Social Science Network, Academia, Google Scholar, and searches on relevant NGO (Non-Governmental Organisation) websites were used as the primary search engines for the grey literature.

Part-I Books, Policy Guides, Discussion Papers, Reports

Hossein Bidgoli's[6] book is a comprehensive work on Electronic Commerce that mixes descriptive information about the internet and electronic commerce with practical applications and actual case studies. Among important issues covered are intranets/extranets, electronic data exchange, electronic payment systems, supply chain management, auctions on the Web, marketing and advertising on the Web, new hardware and software technologies, security issues, and building a successful E-Commerce site, as well as personal, social, organizational, legal, and tax issues. The book has examined the balance of theories, applications, and hands-on material. It is divided into four parts: Electronic Commerce Basics, Electronic Commerce Supporting Activities, Implementation and Management Issues in Electronic Commerce, and Appendix and Glossary. The book has emphasised on introductions of leading companies with significant E-Commerce expertise and at least two small case studies.

Yun Zhao's[7] book has examined that the rapid development of electronic commerce has given rise to a new generation of commercial practices and the need to address the issue of resolving disputes arising out of such practices and only recently has attention been paid to this area. The author has raised the issue of dispute resolution that is extremely important because the dispute mechanism used will largely influence the attitudes of merchants and consumers at large, which will in turn determine the fate of electronic commerce. The book provides a comprehensive analysis of the law and practice relevant to dispute resolution in electronic commerce. Anyone interested in E-Commerce Law or dispute resolution, or conducting business over the internet will find this book particularly useful. The work in this book is a milestone in the development of the concept of online dispute

[6] Hossein Bidgoli, *Electronic Commerce, Principles and Practice* (Academics, California, 2002).

[7] Yun Zhao, *Dispute Resolution in Electronic Commerce* (Brill Academic Publishers, The Netherlands,2005).

resolution. In the sixth part of the book author has given the new mechanism for the E-Commerce disputes that is online dispute resolution. It was considered that it might be a bit too early to envisage a perfect and complete dispute resolution mechanism for electronic commerce that would have no gaps, uncertainties, or difficulties, even in developed parts of the world. However, it is considered that the time has come when it should adopt Online Dispute Resolution Mechanism as a part of Dispute Resolution Mechanism.

Alan Davidson's[8] book has examined the laws and regulations involved in Electronic Commerce. The book has addressed the legal issues relating to the introduction and adoption of various forms of electronic commerce. From intellectual property, to issues of security and privacy, author looks at the practical changes for lawyers and commercial parties whilst providing a rationale for the underlying legal theory. In just a few years, commerce via the World Wide Web and other online platforms has boomed and a new field of legal theory and practice has emerged. Legislation has been enacted to keep pace with commercial realities, cyber-criminals and unforeseen social consequences, but the ever-evolving nature of new technologies has challenged the capacity of the courts to respond effectively. The book deals with electronic transactions, internet contracts, domain names, intellectual property, security, evidence, cybercrime and privacy.

Anjali Kaushik's[9] book gives in-depth exposure to the various ways in which security of information might be compromised, how cybercrime markets work and measures that can be taken to ensure safety at individual and organizational levels. The book has examined that Cyber security is not just a technical subject that can be resolved like any other Information Technology related problem. It is a risk that can be mitigated by creating awareness and getting the right combination of technology and practices based on careful analysis. This book combines insights on cyber security from academic research, media reports, vendor reports, practical consultation and research experience. The book discusses motivation and types of cybercrimes that can take place and the major types of threats that users might encounter. It is also discussed the impact, trend and role of the government in

---

8 Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press, New York, 1st edn., 2009).

9 Anjali Kaushik, *Sailing Safe in Cyberspace* (SAGE Publication Ltd, London 1st edn.,2013).

combating cybercrime. The last section of the book examines the ways to protect them and secure their data/information stored in computers and the cyberspace. It concludes by offering suggestions for building a secure cyber environment.

Majid Yar's[10] book has examined that Criminology has been rather slow to recognise the importance of cyberspace in changing the nature and scope of offending and victimisation, and a comprehensive introductory textbook on cybercrime and its social implications is long overdue. One of the many strengths of book is that it avoids 'techy' jargon and unites criminological and sociological perspectives in discussions of cybercrime, cyber-deviance and cyber-freedoms. The book explains the causes many criminologists to feel out of their depth (or at least their comfort zone).

The book provides a clear, systematic, critical introduction to current debates about cybercrime. It locates the phenomenon in the wider contexts of social, political, cultural and economic change.

Michael Shaw's[11] book has examined the electronic exchange mechanisms of the emerging digital economy. It is the New Era of E-Commerce. Electronic Data Interchange (EDI) over Wide Area Networks is beginning to transform the economies of the developed nations. In addition, the internet, and especially the World Wide Web, is contributing to this transformation in an important way. The authors of the book examine the broad scale impact of digital technology on commerce. This book contains and explains to the Security, Privacy, and Legal issues. The internet is inherently an insecure network, although it is becoming more secure. However, the rise of E-Commerce on the internet offers financial incentives to exploit its lack of security, both by interfering with transactions (i.e., reading, tampering, spoofing, and repudiating) and by gaining unauthorized access to organizational networks (i.e., intranets and extranets). E-Commerce also presents legal issues, including the nature of electronic contracts.

---

10 Majid Yar, *Cyber Crime and Society* (SAGE Publications, London, 1st edn., 2006).

11 Michael Shaw, Robert Blanning Troy Strader , *et.al.* (eds.), *Handbook on Electronic Commerce* (Springer, Verlag Berlin Heidelberg, 1st edn.,2000).

Merrill Warkentin's [12] book addresses managerial and research issues related to all aspects of B2B E-Commerce. The 13 chapters of this volume cover the environment of B2B E-Commerce, supply chain management issues, value chain networks, and related research issues in three sections. Topics have been included EDI, exchanges, trust, manufacturing connectedness, automated tendering, virtual alliances, and networks. The chapters are lively, with examples from industry. They also provide new scholarly perspectives on these important new markets and the processes that create and support them.

Lorna E. Gillies's[13] book is based on the theme of three-fold. The first aspect to this book's theme is that consumers should be provided with the substantive and juridical protection of their own law in a contractual dispute with the seller i.e. international private law rules should provide juridical protection for consumers by ensuring any dispute with a foreign seller can be heard in the consumer's jurisdiction and the law of the consumer's domicile applies, thereby facilitating maximal consumer protection. International private law rules already provide juridical protection for consumers via special rules of jurisdiction, choice of law and the recognition and enforcement of judgments. The aim of international private law is premised on a desire to do justice to the parties involved in a cross-border dispute. This aim is particularly significant with regard to the role of international private law vis-à-vis the legal regulation of cross-border electronic consumer contract disputes.

Henry C. Lucas's[14] book presents an approach for analyzing and developing business strategy for electronic commerce and the internet. The first part of the book discusses strategy and new business models. The second part of the book looks at the internet strategies of traditional firms. Despite the publicity about dot.com startups, by far the largest number of businesses in the United States and the world are traditional. They existed long before the internet and electronic commerce.

---

12 Merrill Warkentin, *Business to Business Electronic Commerce: Challenges and Solutions Lorna* (Idea Group Publishing, 1st edn., 2002).

13 Lorna E. Gillies, *Electronic Commerce and International Private Law: A Study of Electronic Consumer Contracts* (Ashgate Publishing Limited, England, 1st edn., 2008) .

14 Henry C. Lucas, *Strategies for Electronic Commerce and the Internet* (The MIT Press Cambridge, Massachusetts London, England,1st edn., 2002).

Gary P. Schneider's[15]book analyses introduction to Electronic Commerce, which defines electronic commerce and describes how companies use it to create new products and services, reduce the cost of existing business processes, and improve the efficiency and effectiveness of their operations. The book addresses Technology Infrastructure: The internet and the World Wide Web, introduces the technologies used to conduct business online, including topics such as internet infrastructure, protocols, and packet-switched networks. It also describes the markup languages used on the Web (HTML and XML) and discusses internet connection options and tradeoffs, including wireless technologies. The book highlights revenue models that companies are using on the Web and explains how some companies have changed their revenue models as the Web has matured. It is explained about internet marketing and online advertising. It includes coverage of market segmentation, technology-enabled customer relationship management, rational branding, contextual advertising, localized advertising, viral marketing, and permission marketing. Lastly, the book discusses security threats and countermeasures that organizations can use to ensure the security of client computers, communications channels, and web servers. The chapter emphasizes the importance of a written security policy and explains how encryption and digital certificates work.

Farooq Ahmad's[16] book has critically examined the provisions of The Information Technology Act, 2000 and analyses the scope of electronic commerce in the light of The Information Technology Act, 2000 and Indian Contract Act, 1872. It is examined interplay of domain name disputes and trademark law, service provider's liability for copyright infringement, defamation and pornography and cyber crimes. The Information Technology Act, 2000 has limited scope. It does not cover all the issues, which have cropped up by the introduction of internet. While going through harmony and it is quite possible that practical difficulties in applying these provisions will ensure in the near future. The machinery to prevent cyber crimes is not well equipped. The cyber appellate tribunal is a one man commission, having law degree an essential qualification.

---

15 Gary P. Schneider, *Electronic commerce* (Course Technology, Cengage Learning, 9th edn.,2011).

16 Farooq Ahmad, *Cyber Law in India* (New Era Law Publication, 4th edn., 2013).

Apostolos Ath. Gkoutzinis's[17]book has addressed that The European Union has long sought to create a single financial area across Europe where consumers in one country benefit from financial markets and activities in other countries. With the emergence of the internet as a platform for the provision of online banking services, the creation of a pan-European market for banking services appeared a realistic proposition. In practice, however, this has not happened. This book asks why and argues that the creation of banking markets via the internet relies on both available technologies and appropriate laws and regulations. The institutional and legal framework for online banking services in the single European market are examined, as is the level of legal harmonization achieved in the UK, France and Germany under the influence of the EU Directives pertaining to online banking activities**.**

Rahu Maltan's[18]book has attempted to answer the Indian Government who had only just announced its policy to allow private citizen's access to the internet. The author in what was being called India's answer to Silicon Valley, he already had a more than nodding acquaintance with companies engaged in software related activities and their peculiar legal problems and so, in a limited way, found himself able to answer these questions on the basis of general principles of law. But with the implementation of new policies, and as more and more entrepreneurs began to muddy their hands in the internet waters, author found being called upon to answer harder, more obscure questions, on all aspects of the law relating to computers and the internet. Not surprisingly, author received no assistance whatsoever, from traditional sources of Indian law. The book attempts to fill this gap. Given the paucity of legal sources within the country, a lot of the issues raised and discussed in this book are issues that were and still continue to be faced by lawyers and lawmakers alike in other countries of the world. This book has analyzed these issues and their probable treatment in the hands of the Indian judiciary in the absence of any judicial assistance.

Talat Fatima's[19] book analyses the legal complexities which arise due to the presence of an array of foreign components on the entire cybercrime scene. It also

---

[17] Apostolos Ath. Gkoutzinis, *Internet Banking and The Lawin Europe, Regulation, Financial Integration and Electronic Commerce* (Cambridge university, 1st edn., 2006).

[18] Rahu Maltan, *Law Relating To Computers And Internet* (Butterworths India, New Delhi, 1st edn.,2000).

[19] Talat Fatima, *Cybercrimes* (Eastern Book Company, Lucknow, 1st edn., 2011).

analyses the vulnerabilities in the transient regime of cybercrimes as these elusive crimes present unprecedented challenges to the legal world. It studies issues as to how these transnational crimes have thwarted the established lex loci delicti rule of jurisdiction and how the anonymity factor pulls back the job of a law enforcer. The present information boom has changed the legal mindset and attempts in this book are directed towards identifying the criminal infractions online, the legal issues involved in tackling it and exploring the legal measures for the arraignment of cyber criminals.

The book is divided into nine chapters. Chapter one, entitled The Communication Story, introduces to the reader, the background in which the entire online activity is carried on and the infringers who commit crimes and other acts of vandalism. Chapter two, entitled Nature of Cybercrimes, briefly introduces the novel topic of cybercrimes, traces the crime concept in the primitive society and its journey to the present day information society. Chapter three entitled Taxonomy of Cybercrimes: All Overview, chalks out the typology and conceptualization of cybercrimes by highlighting the difficulties defining elusive crimes. Chapter four entitled Pure Cybercrimes, which are the typical form of cybercrimes, are the subject-matter of this chapter. The vandalizing of digital information, challenges the integrity of computer systems and the introduction of certain malicious programs and codes which result in the breach of security and privacy.

Chapter seven, entitled Legal Issues Involved in Countering Cybercrimes, discusses the legal complexities in prosecuting cyber criminals. The critical impediments are jurisdictional issues, enforceability issues and evidentiary issues which form the centre of discussion of the present chapter. Chapter eight entitled Cybercrimes: Prevention and Enforcement Strategies, enumerates the various legal measures taken to prevent and control cybercrimes. Chapter nine, entitled An Introduction to the Information Technology Act, 2000, is fully devoted to the cyber legislation of India. It highlights and analyses the recent amendments made in 2008 which can go a long way in checking cybercrimes and evaluating the changes and making valuable recommendations in the field of cybercrimes.

Vakul Sharma's[20] book analyzed impact of The Information Technology Act, 2000 on Regulation of E-Commerce and attempts to make understood in relation with other Codes, Acts, rules and regulations. The Act is now a 'happening Act'- most of the rules and regulations prescribed under the Act have already been notified, Adjudicating Officers are being appointed, the Cyber Appellate Tribunal is now a reality. The author has made an honest attempt to disseminate knowledge about the information technology law by highlighting the legislative spirit behind the enactment of Information Technology Act, 2000.

The book has been divided into two parts: part one is a commentary on the Act. It is a commentary with a difference each and every section, subsection, clause and sub-clause of the Act has been critically analyzed with the help of numerous illustrations, concept notes and examples. The emphasis is on looking at the practical application of law to interpret the true legislative intent behind the Act by referring and applying the supreme Court judgments for better assimilation and understanding of its various provisions.

Part two of the book looks at global issues involved, whether it is the question of jurisdiction, defamation, freedom of expression, electronic taxation or intellectual property rights. Moreover, these global issues have been discussed against the backdrop of emerging case law and enactments. The emphasis is more on deciphering the key legal issues and principles keeping in view the global context of internet. Celebrated cases, like Pinochet, "yahoo', Napster, DeCSS, and Sex.com have been discussed in detail to-bring rut the subtleties and nuances of emerging legal principles in Information 'technology. To make things further understandable, line diagrams, drawings, and comparison charts are being used. An attempt has also been made to include the 'Indian' perspective while discussing the global issues.

Sujeet Kumar's[21] book has dealt with Cyber law that encapsulates the legal issues related to use of communicative, transactional, and distributive aspects of networked information devices and technologies. The book examines that some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction. Issues of jurisdiction and sovereignty have quickly come to the fore in

---

[20] Vakul Sharma, *Information Technology Law and Practice* (Universal Law Publication Co.,1st edn., 2004).

[21] Sujeet Kumar, *Encyclopaedia of Cyber Laws* (ABD Publishers, New Delhi, 1st edn., 2011).

the era of the internet. The book has analyzed that the internet does not tend to make geographical and jurisdictional boundaries clear, but internet users remain in physical jurisdictions and are subject to laws independent of their presence on the internet. The book has examined that Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although, jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extraterritorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic, as the medium of the internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application, and such questions are generally a matter of conflict of laws, particularly private international law. The book has highlighted on the issue of the contents of a web site are legal in one country and illegal in another, in the absence of a uniform jurisdictional code, legal practitioners are generally left with a conflict of law issue. This book has provided deep insight to various dimensions of issues relating to the subject.

Tabrez Ahamad's [22] book has attempted to explore the evolution and development of Information Technology and its threats and opportunities in conducting E-Commerce and M-Commerce transactions. The book has critically examined the IT Act, 2000 and the requirement of broader policy and legal framework to control and regulate the internet. The book examines how the information superhighway gateway is misused in various ways to do cyber crimes, software piracy, invasion of right to privacy, cyber squatting and Examines the requirement of security policy and legal frame work to regulate internet. Author in this book attempts to justify the growth of E-Commerce that has propelled the need for vibrant and effective regulatory mechanism to further strengthen the legal infrastructure so crucial to the success of E-Commerce and M-Commerce. The book deals with technology create new opportunities as well as it poses new challenges. With the emergence of internet and increasing use of the World Wide Web possibilities of infringement of copyright have become mind boggling. The continued rapid evolution of number of key technologies and convergence of broadcasting media, communication media, home electronics, and publishing on computers,

[22] Tabrez Ahamad, *Cyber Law E-Commerce and M- Commerce* (A.P.H. publishing corporation, 1st edn.,2003).

business through electronic media and mobile technologies giving rapid socio-economic development but it is also creating a lot of legal issues.

R.K.Chauey's[23] book has emphasised on right to privacy in digital age and provided new tools in the hands of eavesdroppers. It has also been emphasised on Computers and the internet can be used to amass huge amount of data regarding people, profile it in various ways, modify it and deal with it in a manner which could violate individual's privacy. The author has examined the concept of privacy in the light of various national and international laws. It is discussed how the practices commonly used on the internet like cookies, web bugs, spamming could lead to the violation of privacy. Also, he has highlighted the importance of adopting privacy policy by websites. Cyber crime is the latest type of crime which affects many people. It refers to criminal activity taking place in computer networks, knowingly or intentionally, access without permission, alters, damage, deletes and destroys the database available on the computer or network. It also includes the access without permission to the database or programme of a computer or network in order to devise or execute any unlawful scheme or wrongfully control or obtain money, property or data. It poses the biggest challenge for police, prosecutors and legislators.

V.D.Dudeja's [24] book has emphasised on the interplay of freedom of expression and the internet. The reasonable restrictions on the freedom of expression can be imposed in the interests of privacy and security. Some restrictions can be put on the use of computers and internet because law has been able to recognize computer as a weapon of offence as well as a victim of crime the as emerging cyber jurisprudence. The book has critically examined that Cyber crime is the most recent type of crime, which affects many people. This is the biggest challenge for police, prosecutors and lawmakers. The criminal provisions deal with offences such as tampering with source code, hacking into computer systems, publishing of obscene information and misuse of licenses and digital signature etc. Government efforts are being made in India and abroad to stop such crimes and looks closely on their success and failure. Cyber laws cover these special enactments, which are specially designed to govern or apply to cyber space for example, the Electronic Commerce

---

[23] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* (Kamal Law House, Kolkata, 1st edn., 2008).

[24] V.D.Dudeja, *Cyber Crimes And Law: Cyber Crimes and Law Enforcement* (Commonwealth, 1st edn., 2002).

Act on the Uniform Computer, Information Transaction Act and the Uniform Electronics Transaction Act recently approved in the US.

V.D.Dudeja's[25]book has dealt with International perspectives on computer related crimes, Criminal offences, Internet related crimes, the world wide web and legal resources, Cyber terrorism and its network, Menance of virus, Intellectual property rights and law, Privacy and its legal safeguards, E-Contract and law, Evidence and law, Electronic banking and legal support, Bank related crimes, Frauds and scams, cyber crime-robberies and its prevention, Understanding forged and digital signatures, Hackers, crackers and whackers attack, threat to information systems and security, cyber consumers and E-Commerce, Net work security, Integrating cyber crime and law. The book examines how our current contract laws could be applied to such contracts. The Information Technology Act 2000 is being implemented in India. The regulation could halt the growth of technology just as the lack of clear and consistent law hinder progress. Thus, a fine balances to be achieved between the two with due care and consideration.

Nandan kamath's[26] book examines the various aspects of cyber law and regulation that mentions the legal policies. The topics covered in this book are copyright liability and rights of domain names, right to privacy, security updates, etc. The legal policies in the book are included in the Information Technology Act, 2000 and the new legislations.

In recent times, the internet has emerged as a medium with immense potential, posing many new and interesting challenges. It is not surprising that there have been many attempts to regulate and control this medium, especially through the use of laws and regulations. This exciting publication explores the various aspects of cyber law and cyber regulations, taking the reader through a multitude of legal and policy issues that the Information age pose. Topics covered in this book range from evidentiary aspects and digital signatures to intellectual property concerns such as copyright liability and rights in domain names; from cyber crime and cyber porn to the regulation of free speech on the Net and the right to privacy. Employing a comparative law approach not only takes into consideration the changes brought

---

[25] V.D.Dudeja, *Cyber Crimes and Law: Crimes in Cyber Space; Scams and Frauds* (Commonwealth Publishers, 1st edn., 2002).

[26] Nandan Kamath, *The Law Relating to Computers, Internet and E-Commerce* (Universal Law Publication Co.2nd edition 2000).

about by the Information Technology Act of 2000, but also contains the latest developments along with a comprehensive guide to this legislation.

Alan Davidson's[27] book examines the laws and regulations involved in electronic commerce. Legislation has been enacted to keep pace with commercial realities, cybercriminals and unforeseen social consequences, but the ever-evolving nature of new technologies has challenged the capacity of the courts to respond effectively. This book addresses the legal issues relating to the introduction and adoption of various forms of electronic commerce. From intellectual property, to issues of security and privacy, Alan Davidson looks at the practical challenges for lawyers and commercial parties while providing a rationale for the underlying legal theory.

Gupta, Agarwal [28] the author aims at apprising how the unwary and unscrupulous customer of internet service is duped by expertise of professional criminals and white-collar are tracked down by the wonderfully sophisticated computers. The author has simplified the technical language promoting investigation and prosecution agencies and has given a ready reference with the upcoming law. The Author has thrown light on the loopholes in Information Technology Act, 2000 making it easier for the investigating and defending agencies to have knowledge in different fields of law so as to have solutions. This book shows the practical loopholes faced by investigating agencies in cyber crime laws. Hence, I as the researcher selected this book for my study.

Part-II Papers and Articles

C.M. Abhilash[29] throws light on UNCITRAL Model Law and the basis for passing of the Information Technology Act, 2000. It was the decision of the UNCITRAL to formulate model legislation on electronic commerce .India adopted to enact the one statute called Information Technology Act, 2000.The author has very clearly given the overview of the Indian Law and the legal recognition for digital signatures and the need to have E-Governance. The Information Technology

---

27 Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press, New York, 1st edn.,2009).

28 Gupta, Agarwal, *Information Technology Law and Practice* (Premier Publishing Company, 1st edn., 2009).

29 C.M. Abhilash, "E-Commerce Law in Developing Countries: An Indian Perspective" 11(3 *) Informationand Communication Technology Law* (2002).

Act,2000 upholds the spirit of UNCITRAL Model Law. It further states that there must be proper training of government staff and enforcement personnel.

Rajiv Arora, D.K. Banwet[30] addresses that Electronic commerce is a vital part of India's trade facilitation policy. Following major initiatives in liberalization in 1991 the need to facilitate international trade through policy and procedural reforms has become the cornerstone of trade and fiscal policies. Electronic commerce, including electronic data interchange (EDI), has been implemented in various organizations in India, in particular those that are closely involved in international trade. It is known that the level of electronic commerce development in the organizations has been either facilitated or inhibited by various factors. In order to identify these factors an empirical study comprising a questionnaire combined with case studies and in-depth interviews in selected organizations was carried out. In this article, the results indicate that factors primarily intrinsic to the organizations and organization-driven strategies have been more significant causal factors than either network-driven strategies or factors extrinsic to the organizations in the implementation of E-Commerce in India.

Ihab A. Ismail, Vineet R. Kamat[31] examines that E-Commerce is steadily becoming a reality in the construction industry. However, despite the increasing rate of utilization by owners and contractors alike, the legal implications of using E-Commerce in construction have not been studied in depth. This paper fills this gap in literature. It identifies and analyzes the different types of legal risks involved in the use of e-commerce in construction. It also outlines the risk that contractors and professionals may face in their E-Commerce implementations. A classification of E-Commerce legal risks is also introduced. The legal risks discussed include agency, jurisdiction, contract formation, validity and errors, authentication, attribution, non repudiation, privacy, conflict of laws, and conflict between law and technology.

---

30 Rajiv Arora, D.K. Banwet, "E-Commerce Implementation in India: A Study of Selected Organizations" 10 (1) *Asia-Pacific Development Journal* (June, 2003).

31 Ihab A. Ismail, Vineet R. Kamat, "Evaluation of Legal Risks for E-Commerce in Construction" *Journal of Professional Issues in Engineering Education and Practice* (October, 2006).

Shweta Sharma, Sugandha Mittal [32] addresses that E-Commerce has unleashed yet another revolution, which is changing the way businesses buy and sell products and services. E-Commerce stands for electronic commerce and pertains to trading in goods and services through the electronic medium. India is showing tremendous growth in the E-Commerce. The low cost of the Personal Computer and the growing use of the internet is one of reasons for that. There is a growing awareness among the business community in India about the opportunities offered by E-Commerce. The future does look very bright for E-Commerce in India with even the stock exchanges coming online providing an online stock portfolio and status with a fifteen-minute delay in prices. In the next 3 to 5 years, India will have 30 to 70 million internet users which will equal, if not surpass, many of the developed countries.

Pradeep Kaur, Mukesh M Joshi[33] deal with Commerce is a communicative transaction between two parties playing very familiar roles: buyer and seller. For commerce to occur, somebody must do the selling, and somebody must do the buying, and these two some bodies must share a basic understanding of how the transaction is generally supposed to flow. Electronic commerce, commonly known as E-Commerce or E-Commerce, consists of the buying and selling of products or services over electronic systems such as the internet and other computer networks. The amount of trade conducted electronically has grown dramatically since the spread of the internet. A wide variety of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, internet marketing, online transaction processing, Electronic Data Interchange (EDI), automated inventory management systems, and automated data collection systems. In this paper, author has discussed the structure of E-Commerce along with its advantages and challenges.

Subhajit Basu, Richard Jones[34]'s focus on India, a rural economy where E-Commerce is set deal with the problem in today's Indian producer/consumer chain,

---

[32] Shweta Sharma, Sugandha Mittal, "Prospects of E-Commerce in India" *available at: http://*www.rimtengg.Comiscetproceedingspdfsadv _Nw_Tech43 .Pdf (last visited on March 1, 2013).

[33] Pradeep Kaur, Mukesh M Joshi "E-Commerce in India: A Review" 3(1) *International Journal of Computer Science and Technology* (January-March 2012).

[34] Subhajit Basu, Richard Jones ," E-Commerce and The Law: A Review of India's Information Technology Act, 2000"12(1) *Contemporary South Asia* (2003).

that is the middlemen (powerful distributors), who make most of the money, while the poor producer gets a pittance. E-Commerce has the potential to change this scenario dramatically and it is beyond question that there is a need for a coherent yet flexible legal network to felicitate the e-entrepreneurs spirit and the confidence of consumers. The Information and Technology Act, 2000 is India's attempt to formulate such legal network. It is our view that the Act is too prescriptive. The attempt to relate to particular forms of technology and to foresee all possible options has created an over complex set of provisions that will hinder rather than encourage the development of E-Commerce.

C Satapathy[35] critically examines the Taxation issues relating to electronic commerce which are not confined to customs duties alone. Equally important concerns arise in relation to domestic taxes such as sales tax, value added tax and income tax relating to sale of products over the internet. It is no small challenge to experts in taxation, law and economics to design an equitable tax system for electronic commerce.

S.Sai Sushanth[36] highlights that the traditional way of transacting business is replaced by electronic commerce popularly known as E-Commerce. E-Commerce means using of information technology, computers and other electronic means to transact business by and between individuals and entities. E-Commerce is one of the significant developments in the International Trade. It has provided many advantages besides many challenges. The Information Technology Act, 2000 is one of the primary laws, which has promoted E-Commerce, E-Governance and has provided legal recognition to e-records and e-transactions. Cyber law in India tires to attend these challenges and requires compliance of The Information Technology Act, 2000 Laws by business houses engaging in ecommerce. The Indian Information Technology Act, 2000 make it mandatory to set up corporate compliance programs including cyber law compliance program.

---

[35] C Satapathy, "Taxing Electronic Commerce," *Economic and Political Weekly* (May 9, 1998).

[36] S.Sai Sushanth, "E-Commerce and Law:Trends and Challenges" 3(2) *UACEE International Journal of Advances in Computer Science and its Applications* (2013).

Suneeti Rao[37] deals with The Information Technology Act, 2000, aimed particularly at encouraging the growth of E-Commerce, fails to satisfy the basic precondition for such growth as building trader and consumer confidence. At this stage in the growth of the industry consumer protection is far more important than protection for technology developers and promoters. The absence of representation of consumer bodies or departments dealing with consumer affairs in the various bodies which drafted the act is evident in the biases in the act.

C Satapathy[38] focuses on adequate legal framework in place and rapid technological advances in the field of Secure Electronic Transactions, global electronic commerce will grow rapidly and create new opportunities for trade that no nation can afford to miss. So there is an urgent need to legislate our own national cyber laws on the pattern of the UNCITRAL Model Law and to formulate necessary subsidiary regulations.

C Satapathy[39] deals with a possible negotiating strategy on E-Commerce at the Doha Ministerial for developing countries such as India which, despite typical infrastructural weaknesses, have demonstrated a strong growth potential in e-exports.

Subhajit Basu, Richard Jones[40] focuses on which will significantly impact the global economy and play a vital part in future economic development. Europe and the United States are currently seen as the main beneficiaries of such growth, but countries such as India and China with their huge pools of technologically skilled manpower have exceptional opportunities. A number of developing countries have pursued policies to formulate a consistent legal and regulatory framework to support electronic transactions across state, national and international borders. The development of the appropriate legal framework has required substantial re-thinking of traditional legal approaches. Many legal rules assume the existence of paper records, documents, signatures, physical cash, cheques, face to face meetings, and so on. As more transactions are carried out by electronic means, it becomes important

---

37 Suneeti Rao, "Information Technology Act: Consumers' Perspective" *Economic and Political Weekly* (September 15, 2001).

38 C Satapathy " Legal Framework for E-Commerce" *Economy and Political Weekly* (18 July 1998).

39 C Satapathy "WTO Work Programme on E-Commerce Strategy for Further Negotiations" *Economic and Political Weekly* (September 29, 2001).

40 Subhajit Basu, Richard Jones "E-Commerce and the Law: A Review of India's Information Technology Act, 2000" 12(1) *Contemporary South Asia* (2003).

that evidence of these activities be available to demonstrate the ensuing legal rights and obligations. India's Information Technology Act, 2000, provides a legal framework so that transactions are not denied legal effect, validity or enforceability solely because they are in electronic form. In this paper, we will outline the economic impact of E-Commerce on the developing countries and review the main provisions of the Information and Technology Act 2000 in the context of contractual, jurisdictional, security, and regulatory issues. The Act will be contrasted with similar provisions in Europe, the United States and South East Asia.

Annet Wanyana Oguttu, Mrs Sebo Tladi[41] deals that it is a principle of international tax law that a country may not tax the business profits of a non-resident enterprise unless those profits are attributed to a "permanent establishment" located in the source country. A "permanent establishment" is defined as a fixed place of business through which the enterprise is wholly or partly carried on. The "business establishment" concept is however based on the world where there had to be a physical presence of the business in order for its profits to be taxed. The requirement of a fixed place of business faces challenges when trade is conducted electronically as E-Commerce makes it difficult to identifying a taxable presence in the source country. This article analyses the challenges that E-Commerce poses to the "permanent establishment" concept.

Sylvia Mercado Kierkegaard[42] has explained that The United States (U.S.) and the European Union (EU) offer contrasting approaches to contract formation in Cyberspace. Two foci can be identified with EU law: (1) consumer protection and (2) market harmonization. The American approach, however, is characterized by self-regulation and economic rationale. Author examines and compares the EU and U.S. regulatory approaches to electronic contracting.

---

41 Annet Wanyana Oguttu, Mrs Sebo Tladi, "The Challenges E-Commerce Poses to the Determination of a Taxable Presence: The Permanent Establishment, Concept Analyzed from a South African Perspective" 4(3) *Journal of International Commercial Law and Technology* (2009).

42 Sylvia Mercado Kierkegaard, "E-Contract Formation: U.S. and EU Perspectives"12 *Shidler Journal Law Company and Technology* (2007).

Sarabdeen Jawahitha, Noor Raihan Ab Hamid[43] addresses that the World Wide Web (www) has brought new opportunities and challenges to various people. The businesses utilize it for their benefit by expending their activities not only in physical space but also in virtual space in search of the potential customers. Thus, contracting becomes a fundamental element in E-Commerce world. The electronic contracting raises various new legal issues. The general inclination of the legislature and the legal profession is to apply the existing law to the new sets of virtual commerce problems without much change; even where modification is necessary or unavoidable to protect the interest of e-businesses and e-consumers. This paper seeks to analyze, inter alia, general principle of contracts, forms of electronic contracts, moments of formation of contract, along with the applicability of principles of click wrap agreement and digital signature in an E-Contract in comparison with the Hong Kong, United Kingdom, United State statutes and European Union's Directives on E-Commerce.

9. Chapter-Wise Introduction

In addressing the issues specified above, the study is organized into five chapters

Introduction

Chapter 1 - The E- Commerce in India: An Analysis

This chapter deals with not only the meaning and concept of E-Commerce in India but also development and classification of E-Commerce in Indian perspective. It also describes several key element of E-Commerce such as encryption, security, data protection and digital signature in which it is explained the payment instrument used through light on the protection on Intellectual Property on the internet as well as attempt to describe situation of taxation in India.

Chapter 2- Regulatory Framework of E- Commerce in India

This chapter will explore the emerging national and international legal framework of regulation relating to E-Commerce in India in which relevant provision of The Information Technology Act, 2000 and latest amendment will be dealt

[43] Sarabdeen Jawahitha, Noor Raihan Ab Hamid, "Electronic Contract and The Legal Environment" *available at: http://* www.irfd.org/events/wf2003/ papers_global/R38.pdf (last visited on February 15, 2013).

concerning cyber E-Commerce. This chapter will highlight the Concept Attribution, Time and Place of Dispatch and Receipt of Electronic Data. It also describes the legal regulation of several certifying authorities, which shall be helpful to regulate and boost up E-Commerce in India.

Chapter 3 - The Electronic Contract under Digital Technology

This chapter will describe the meaning and essential ingredients of electronic contracts which will determine its scope. It also deals with the kind of electronic contract including with the evidentiary value of electronic contract. This chapter will explain how consumer protection issue in electronic contract to be resolved. This chapter contains relevant provision of The Information Technology Act, 2000 related to Electronic Contract.

Chapter 4 - The E-Commerce: Crime and Jurisdictional Issues on Internet

This chapter will describe the concept and classification of Cyber Crime in which several provision of The Information Technology Act, 2000 will be dealt. It will help in preventing Cyber Crime concerning E-Commerce in India. This chapter will explore emerging dimension of jurisdiction in Cyber Space in which jurisdictional principles under National and International law. It also describes that how jurisdictional issue in cyber space might be resolved.

Chapter 5- E-Commerce and International Regulations

This chapter will explore the emerging international legal and institutional framework for regulation of E-Commerce. The international law related to E-Commerce and conventions play an important role in harmonizing national substantive legal norms, as well as procedural rules. This chapter deal several treaties and convection such as United Nation Convention on International Trade Law, European Electronic Commerce Directive, Uniform Electronic Transaction Act, World Intellectual Property Organization, World Trade Organization, and Indian legislation: The Information Technology Act, 2000.

Chapter VII: Discussions, Conclusions and Recommendations

The Researcher presents certain recommendations and suggestions by which the Government, the appropriate authorities and other stakeholders would be benefited.

CHAPTER I

E-COMMERCE IN INDIA; AN ANALYSIS

Introduction

The legal aspects or issues related to any activity of citizens in cyberspace come within the ambit of cyber law. E-Commerce means the paperless exchange of business information using a suite of technologies such as Electronic Data Interchange (EDI), Electronic Mail (e-mail) Electronic Fund Transfer (EFT), Credit Cards, Fascimile (Fax), Electronic Bulletin Board Systems (BBS) and Data Base Services. In other words, E-Commerce is a form of computerized buying and selling both by consumer and by company, which facilitates choosing the goods ordering, delivery, after sales support and payment. An important question whether jurisdiction should be determined by reference to where material originated, where it went along the way or where it ended up being displayed, stored or printed out. It may be said that an infringement has been taken place and under more than one law. There is the problem of choice of law as jurisdiction may arise in number of countries because the law of each country is different. In Indian Law, there does not require compulsory registration of work whereas in United State copyright law requires compulsory registration. There is need of Uniformity of law for smooth functioning of E-Commerce in India.

The researcher will try to address about Tax treatment of such products under various tax levies such as custom, excise, sales tax.etc. pose vexatious questions as well as issues relating to the jurisdiction of taxing authorities. At the time, The World Trade Organization (WTO) proposed to free all electronic transmissions from customs duties about equity in the context of taxing or none taxing a product depending on its mode of delivery. E-Commerce has given the birth of new system of paying for goods and services. It should be noted that this is done through Electronic Fund Transfer (EFT) system such as credit cards e.g. MasterCard, Smartcard. In fact, it is a virtual bearer cheque. This system is advantageous because transaction go direct from site to site in an instant, rather like handing over cash.

These are few complex issues of security, privacy, authentication and anonymity, which have been thrust into the forefront as confidential information

increasingly traverses modern networks. For the functioning of E-Commerce, confidence, reliability and protection of information against security threats are very crucial prerequisite. A security threat may be defined as a crucial condition or event with the potential to cause economic hardship or loss to data or network resources by disclosure, modification of data, denial of service, fraud, waste and abuse. In sum, the fast developing technology innovation in the world of the Wired and Wireless internet require for increasing governance capacity among social, educational and political organization to create an equitable and safe knowledge Society.

1.1. Genesis

E-Commerce originated in a standard for the exchange of business documents, such as orders or invoices, between suppliers and their business customers. This standard had its inception in the 1948–49 Berlin blockade and airlift. The United State Army quickly discovered that the normal manner of transacting business accompanied by paper orders could not keep up with the necessary flow of goods into Berlin. To break the paper bottleneck, Edward A. Guilbert, a logistics officer in the army, set up a system of ordering via telex, radio-teletype, and telephone. Various industries elaborated upon this system in the ensuing decades before the first general standard was published in 1975. The resulting National Electronic Data Interchange (EDI) standard is unambiguous, independent of any particular machine, and flexible enough to handle most simple electronic transactions. With the introduction of the first graphical browser software for accessing the World Wide Web in 1993, and the ensuing scramble for companies and individuals to get online, most E-Commerce shifted to the internet. In some fields, new internet retailers such as the bookseller Amazon.com grew up to challenge the dominance of traditional retailers. Some established companies embraced the electronic commerce model as well.[1]

Electronic communication started with the arrival of telephone interaction audio at the turn of the 20th century. Radio (audio) in early decades of the century and TV (video cum audio) followed it around mid of the 20th century. Then onward, though telephone remained as private medium of communication, TV changed its face from black- and-white to colour. However, during 1980s cable TV started picking up

[1] Encyclopedia Britannica Online Academic Edition., *available at*: *http://*www.britannica. com/ EBchecked/topic/183748/E-Commerce (last visited on February 12, 2014).

its place the world over, during the same period telephone line had been used as facsimile for transferring data /image. The National Physical Laboratory in Britain set up the first network along these principles in 1968. The Pentagon followed with a larger and more ambitious project in 1969. The first node was established at the University of California (Los Angeles), followed by three others. This mini-network was named ARPANET (Advanced Research Project Agency NET hereinafter referred to ARPANET) and its primary aim was to enable transmission of data files and long distance computing, including accessing data and research files at distant sites.[2]

In 1972, the first electronic mail programme was written to allow the distribution of messages across a network. This permitted research collaboration at a distance. With the introduction of mailing lists, like-minded individuals could form groups devoted to the discussion of specific subject. In 1973, the first International connections to ARPANET were established with Britain and Norway. Within a short time, other networks were established and networked through ARPANET. TELNET (a commercial version of ARPANET) came online in 1973. The publication of a Transmission Control Programme (TCP) by Cerf and Kahn was a major breakthrough in standardization and flexibility. It facilitated the rapid growth and development of the ARPANET because the software was freely available in the public domain and could handle many kinds of machines. It was also realized that, just as a telephone would be of little use unless many people had one, linking to the ARPANET would allow the identification of other users. In time, ARPANET became an insignificant part of the internet as more and more networks were established and more and more machines became linked. In 1983, the military component of ARPANET became a separate network called MILNET, now just one network among many hundreds. ARPANET formally expired in 1989, but its demise was scarcely noticed because all its functions continued to be performed at hundreds of sites. Domain Name Servers were introduced in 1984.[3] The significant advance made by our species, the most important is the development of the internet. The Advanced Research Projects Agency Network was seen as a military network of 40 computers connected by a web of link and lines. This network slowly grew and the internet was born. By 1981, over 200 computers were connected from all over the world. Now the figure runs into

---

2 Nandan Kamath, *Law Relating to Computers Internet and E-Commerce* p.3 (Universal Law Publication Co Pvt. Ltd, 2nd edn., 2000)

3 *Id.* at p.3.

millions. The internet came to India in 1985 with the Educational and Research Network (ERNET) project of the Department of Electronics.[4]

Since 1991, after India took major initiatives in liberalization and opening of the economy with a view to integrate itself with the global economy, the need to facilitate international trade both through policy and procedure reforms has become the cornerstone of India's trade and fiscal policies. The era of Electronic Data Interchange (hereinafter referred to EDI) was ushered in with the setting up of the EDI Council in the Ministry of Commerce in 1994. It was the main organization responsible for facilitating international trade. The EDI Council has promoted the introduction of EDI and E-Commerce in the trade processes of various vital trading partners responsible for the regulation and facilitation of international trade. These organizations include the Indian Customs and Central Excise, ports and airports authorities, shipping lines, airlines, facilitating bodies such as the Directorate General of Foreign Trade (DGFT), Agriculture and Processed Food Export Development Authority (APEDA) and Apparel Export Promotion Council (AEPC).[5] In August 1995, Videsh Sanchar Nigam Ltd. (VSNL), a Public Sector Undertaking started offering internet service to individuals. This opened up a hitherto unexplored market.[6]

The internet grew significantly after the introduction of the World Wide Web, through which it became graphical and interactive. The World Wide Web is a network of sites that can be searched and retrieved by a special protocol known as Hyper Text Transfer Protocol (hereinafter referred to as HTTP). This protocol simplified the writing of addresses automatically searched the internet for the address indicated and 'called up' the document for viewing. HTTP was written by Tim Berners-Lee in 1989, but came online only in 1993. Once the dial and retrieve language had been simplified, the next step was to design an improved browser, a system that would allow links to be hidden by text that could be activated by clicking a mouse button. This was done using an extremely user-friendly programming language called Hyper Text Markup Language (hereinafter referred to as HTML), which allowed even

---

4 Rajiv Arora, D.K. Banwet, "E-Commerce Implementation in India: A Study of Selected Organizations" 10(1) *Asia-Pacific Development Journal* pp. 69-70 (June, 2003).

5 *Ibid*.

6 Tabrez Ahamad, *Cyber Law E-Commerce and M-Commerce* pp.3-5(A.P.H. Publishing Corporation, 1st edn.,2003).

comparative novices to write their own individual 'home-page' for external viewing. In the last few years, applications have become available that translate documents written with word processors into HTML, so that web authors need to know very little about hypertext programming.[7]

In addition, browsers such as Netscape, Internet Explorer and Mosaic allow users to access the internet on a global basis and reach the millions of 'web pages' that are currently available, at the click of a mouse button. The technology of the Web with its hypertext linking allows the most unsophisticated user to surf unhindered. The first internet search engine for locating and retrieving computer files, was developed at McGill University (Montreal) in 1990. Search engines such as Altavista.com, Infoseek.com, HotBot.com, Google.com, etc., help to shift through the vast quantities of information available on any given subject on the internet.[8]

The origins of the internet lie in the military domain. The information society of today is the culmination of the electronic development and the invention of communication systems way back towards the end of the 19th century. After passing through prolonged inventory phases stretching over about a century, in the year 1876, the telephone was patented by Graham Bell. This can be termed as the sapling sown by him for the fast moving telephonic global communication system of today about more than a century thereafter. Not only voice communication of yesteryears but also data transmission (through devices like fax machines and computers) comprise the communication world of today.[9]

1.1.1. Phase I-From Telegraph to Telephone to Computer

1.1.1.1. Telegraph

'Telegraph' is the Greek expression, which mean in the English 'To write far'. In this way, the human society saw the first substitute to direct dialogue. The earliest forms of telegraphy were smoke, fire, drum signals often termed as Jungle Telegraph. These were the very first method to say something from a distance. As early as 1500s, the contemporary thinkers had first started deliberating on the use of light and electric impulses as the means of communication. The first crude system was made without

---

7 Nandan Kamath, *Law Relating to Computers Internet and E-Commerce* pp. 4-5. (Universal Law Publication Co Pvt. Ltd, 2nd edn., 2000).

8 *Ibid*.

9 *Ibid.*

electricity, it was a system of semaphores or tall poles in which the messages were conveyed physically using flags or lights but the sound was not easily audible. When Charles Marshall in 1753 sent the Scots Magazine explaining the process of telegraphy through an electric medium, it became the first recorded mention of the use of a telegraph. The telegraphic concept made progress with the invention of the effects of electromagnets in the 19th century. It paved the way for a more advanced electronic communication.[10]

William Sturgeon invented the electromagnet in 1825, which led to an evolution in electronic communication. The earlier non-electronic telegraph invented by Claude Chapped in 1794 was gradually overtaken by the new experiments in the field like the invention by Harrison Dyer who successfully experimented with transmission of electronic sparks through chemically treated paper tape to burn dots and dashes. Joseph Henry developed three telegraph systems based on electromagnet in 1830, by William Cooke and Charles Wheatstone in 1837 and by Samuel Finley Breese Morse who improved Henry's invention. It is Samuel Finley Breese Morse whose famous words "What hath God wrought?" are registered as the first ever successfully transmitted telegraphic message in the history of telegraph sent by him from Supreme Court Chamber in Washington DC to Baltimore on 25th May 1844. Within a few decades thereafter, the first transatlantic cable was laid in 1858 but the successful link was achieved in 1866.[11]

1.1.1.2. Telephone

It was on the historic day of 10th March 1876 when Bell told his assistant sitting in the next room on phone 'Mr. Watson-come here-I want to see you'. The words passed into history of communication as the first talk on phone. This was the successful culmination of Graham Bell's theory, the harmonic telegraph which was based on the principle that several notes could be transmitted simultaneously along the same wire. The quicker but less reliable media, the telephones were just born. At times, telephones had raised the question of evidence in law courts in this respect. They shared the same treatment, which was meted out to the electronic communication until legal provisions were formulated to give them the due

[10] Talat Fatima, *Cybercrimes* p.4 (Eastern Book Company, Lucknow, 1st edn., 2011).
[11] *Id.* at p.5.

recognition.[12]

1.1.1.3. Computers

The birth of computer and the computer law is inexorably intertwined and fixing a date of their origin is difficult. Blaise Pascal who built the first digital but non-electronic computer in 1642 taught to the world the ABC of Computer building. Charles Babbage considered as the father of computers is credited with inventing the first mechanical computer that eventually led to designs that are more complex. He began in 1822, which was called the difference engine. In 1991, a perfectly functioning difference engine was constructed from Babbage's original plan. Herman Hollerith can be credited for contributing towards the development of automated computing when he developed a mechanical tabulator based on punched cards to rapidly tabulate statistics from millions of pieces of data. Machines built by him were used in the 1890 census and was later adopted by the International Business Machines Corporation (IBM) in the early decades of the 20th century.[13]

In 1946, in the University of Pennsylvania, first general purpose engineers built Electronic Computer that was called Electronic Numerical Integrator and Computer (ENIAC). The weight was above 30 short tons. Invention of transistors in 1947 led to the production of faster and more reliable electronic computers. In 1958, Control Data Corporation introduced the first fully transistorized computer designed by Seymour Cray. Miniaturization continued through the 1960s and in 1965s, the first successful commercial minicomputer was launched. Computers at this stage meant mainframe computers. By late 1960s, big businesses started relying on computers and the first Personal Computer was introduced in 1975.[14]

1.1.2. Phase II-From Advanced Research Projects Agency Network (ARPANET) to The Semantic Web

The internet started in a small way in United State (hereinafter referred to as US) in the year 1969 with barely three computers; one in Utah and the other two in California by Advanced Research Projects Agency (ARPA), part of the Department of Defense (DoD) as the basis of its own network-Advanced Research Projects Agency Network (hereinafter referred to as ARPANET), a small network shared by

[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*

supercomputers in US. In early 1970s, ARPANET grew to 23 hosts who were colleagues and researchers. By 1973, the ability to e-mail colleagues went international. By 1981, the number of ARPANET hosts reached 213 and in 1983, the host group protocol of ARPANET was changed from the initial Host-to-Host Protocol, called the Network Control Protocol (NCP) to Transmission Control Protocol (TCP) and Internet Protocol (IP). The following year saw the introduction of the Domain Name System (DNS) as the host database had become so big that it was not possible to store the list of hosts on one computer.[15]

Thus, the Domain Name System (DNS) was created to allow the database to be distributed across numerous individual servers. The US Government shelved ARPANET in 1990 and by then the internet had proliferated as a major infrastructure in the communication world. Exact number of user is beyond common assessment and hence, number of hosts is taken to measure the growth of the internet. The invention of television was made in 1930s (the British Broadcasting Corporation was running the first public television service by 1936) but its real impact on the Western world was not completely felt before 1950s and 1960s and it took two more decades to become a household appliance in India (1980s).[16]

1.1.2.1. Semantic Web

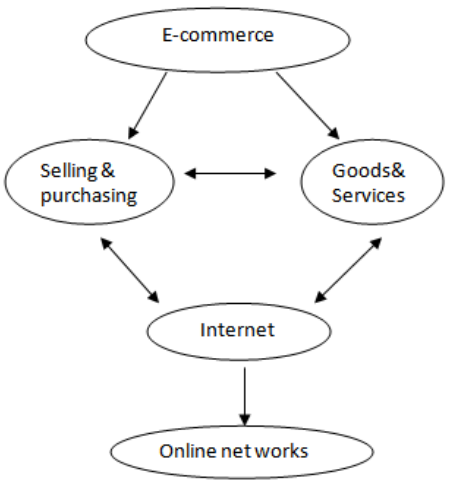
Today the internet is omnipresent. It is gaining popularity equally among academicians, military personnel, businesses, State departments. The Computer, lifeline of the internet, has now become a domestic appliance. Tim Berners-Lee, the father of World Wide Web is the first person who realized that a new form of Web content that is meaningful to computers will unleash a revolution of new possibilities and coined the term semantic web. In a semantic web situation, the computers are envisioned as being more interactive, more responsive. Tim's vision is a Web that allows software agents to carry out sophisticated tasks with ease, making comprehensible connection between bits of information so that computer scan perform more of the tedious work involved in finding, combining and acting upon information on the web.[17]

---

[15] Talat Fatima, *Cybercrimes* p.5 (Eastern Book Company, Lucknow, 1st edn., 2011).
[16] *Id.* at pp.7-10.
[17] *Ibid.*

The entire idea arises from the fact that data embedded in Hyper Text Markup Language (HTML) has only limited use. It cannot be used for purposes other than that for which it is meant. It is with the help of the Resource Description Framework (hereinafter referred to as RDF) processor that semantic technology works. With the use of Uniform Resource Identifiers (URIs) for each of the terms in the language of the user, the matter can be published with more ease. In the opinion of jurist, the semantic web will be solving many legal entangles. Firstly, the fear of the data being stolen, a common complaint today will be mitigated to some extent as only one with a generic RDF processor can use it. Secondly, it will also help the law enforcers in investigating transborder crimes, as conversion of the evidentiary data in the language of the user will be possible. It will ultimately overcome the language barrier in the path of investigators. The computers would not remain as complex and passive as they are today, hence things in the legal arena would start getting easier because it is the strange language machine, which often hampers the Judicial Procedures.[18]

1.2. Meaning and Concept of E-Commerce



The Commerce is a communicative transaction between two parties playing a very familiar role that is buyer and seller. For commerce to occur, somebody must do the selling, and somebody must do the buying, and these two bodies must share a basic understanding of how the transaction is generally supposed to flow. Electronic commerce, commonly known as E-Commerce, consists of the buying and selling of products or services over electronic systems such as the internet and other computer

[18] *Id.* at pp.10-12.

networks.[19] E-Commerce describes the buying, selling, and exchanging of products, services, and information through computer networks, primarily the internet. E-Commerce is changing all business functional areas and their important tasks, ranging from advertising to paying bills.[20] E-Commerce refer to the paperless exchange of the business information using a suite of technologies such as Electronic Data Interchange(EDI), Electronic mail (E-mail), Electronic Fund Transfer(EFT), credit cards, Fascimile (Fax), Electronic Bulletin Board Systems (EBBS) and Data Base Service. In simple terms, E-Commerce is a form of computerized buying and selling both by consumer and from by company, which facilitates choosing the goods, ordering, delivery, after sales support and payment.[21]

With the advent of internet and its commercialization since 1994, a new medium of commerce popularly known as E-Commerce (EC) rapidly emerged in the modern global economy. E-Commerce can be defined as the use of the internet and other networking technologies for conducting business transactions. Further, E-Commerce not only involves selling and buying online but it also involves a host of activities spanning the firm's value chain like promotion of product/services on the web, integrating invoicing and payment from customers, secure transactions, and handling customer queries online. In short, E-Commerce is an umbrella concept to integrate a wide range of existing and new applications.[22]

E-Commerce stands for electronic commerce and pertains to trading in goods and services through the electronic medium, i.e. the internet or phone. On the internet, it pertains to a website, which sells products or services directly from the site using a shopping cart or shopping basket system and allows credit card payments. It involves conducting business with the help of the electronic media, making use of the information technology such as Electronic Data Interchange (hereinafter referred to as EDI). In simple words, Electronic commerce involves buying and selling of goods

---

19 Pradeep Kaur, Mukesh M Joshi, "E-Commerce in India: A Review" 3(1) *International Journal of Computer Science and Technology* p.802 (January-March, 2012).

20 Madan Lal Bhasin, "E-Commerce Payment Systems" 4(1) *chartered secretary* p.45(2007).

21 Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* p.1 (A.P.H. Publishing Corporation, 1st edn.,2003).

22 Sridhar Vaithianathan, "A Review of E-Commerce Literature on India," *available at*: *http://*download.Springer.Comstaticpdf186art%253a10.1007%252fs10660-010-9046-0.Pdfauth66 =1393853765_Ceb2a84f1fc05f57feba8b3b56086344&Ext=.Pdf (last visited on February 1, 2013).

and services over the World Wide Web.[23] Electronic Commerce or E-Commerce consists primarily of the distributing, buying, selling, marketing, and servicing of products or services over electronic systems such as the internet and other computer networks. The information technology industry might see it as an electronic business application aimed at commercial transactions. It can involve electronic funds transfer, supply chain management, e-marketing, online marketing, online transaction processing, electronic data interchange (EDI), automated inventory management systems, and automated data collection systems. It typically uses electronic communications technology such as the internet, extranets, email, e-books, databases, and mobile phones.[24]

Most people think E-Commerce means online shopping. But web shopping is only a small part of the picture. The term also refers to online stock, bond transactions, buying and downloading software without ever going to a store. In addition, E-Commerce includes business to business connections that make purchasing easier for big corporations. E-Commerce is generally described as a method of buying and selling products and services electronically. The main vehicle of E-Commerce remains the internet and the World Wide Web, but use of e-mail, fax and telephone orders is also prevalent. Electronic Commerce is the application communication and information sharing technology among trading partners to the pursuit of business objectives. E-Commerce can be defined as modern business methodology that addresses the needs of the organization, merchants and consumers to cut costs while improving the quality of goods and services and speed of service delivery.[25]

E-Commerce is associated with the buying and selling of information, products, and services via computer networks. A key element of E-Commerce is information processing. The effects of E-Commerce are already appearing in all areas

---

[23] Shweta Sharma, Sugandha Mittal, "Prospects of E-Commerce in India" *available at: http://*www.rimtengg.Comiscetproceedingspdfsadv_Nw_Tech43.Pdf (last visited on March 1, 2013).

[24] S. Sudalaimuthu, J Lilly "Emerging Trend of E-Commerce," *available at*: *http://*www.fibre2fashion.com/industry-article/market-research-industry-reports/emerging-trend-of-E-Commerce-in-india/emerging-trend-of-E-Commerce-in-india1.asp (last visited on February 10, 2010).

[25] Mr Rajiv Rastogi, "India: Country Report on E-Commerce Initiatives" Director Department of Information Technology: Ministry of Communication and Information Technology India, *available at*: *http://* www. unescap.orgtidpublicationpart_ three2261_ind.pdf (last visited on February 2, 2011).

of business, from customer service to new product design. It facilitates new types of information based business processes for reaching and interacting with customers-online advertising and marketing, online, order taking and online customer service etc. It can also reduce costs in managing orders and interacting with a wide range of suppliers and trading and trading partners, areas that typically add significant overheads to the cost of products and services.[26]

Electronic Commerce or trading through the internet has become a reality. Any deal involving the transmission of electronic signals can be classified as Electronic Commerce. The internet's unique ability to allow a company's marketing message to have a global reach and selectively target those consumers already predisposed towards actual purchase of the product, has spurred a rush among corporations both large and small, to set up shop on the internet.[27] E-Commerce encompasses all business conducted by means of computer networks. It reflects a paradigm shift driven by two primary factors: a wide range of converging technological developments and the emergence of the so-called 'knowledge economy'. Recent advances in telecommunications and computer technologies have moved computer networks to the centre of the international economic infrastructure, and everyone with a computer and connected to the internet has become a potential player and a potential market for the e-entrepreneur. These technological developments have gone hand in hand with a trend, predominantly in the developed world, towards a post-industrial knowledge economy.[28]

Just as the industrial society built on and then dominated the agricultural society, the knowledge society is now building on the platform provided by the industrial society. It can be argued that E-Commerce is the first real manifestation of the knowledge society along with the technologies and knowledge required to affect it. The question for the less industrialized developing countries is whether they can use appropriate technologies to leapfrog into the knowledge society, bypassing some of the stages of the industrial paradigm. The vast majority of these E-Commerce transactions to date have taken place in countries with advanced economies and infrastructure. For developing countries such as India, E-Commerce offers significant

---

[26] *Ibid*.

[27] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.781 (Kamal Law House, Kolkata, 1st edn., 2008).

[28] *Ibid.*

opportunities. E-Commerce diminishes existing advantages of cost, communication, and information, and may create huge new markets for indigenous products and services. While many companies and communities in India are beginning to take advantage of the potential of E-Commerce, critical challenges remain to be overcome before its potential can be fully realized for the benefit of all citizens.[29]

Electronic transactions are conceptually very similar to traditional (paper-based) commercial transactions. Vendors present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payment. Then vendors deliver the purchased products. While the precise order of these events and the mechanisms through which they are transacted vary, these activities are in principle, fundamental to both traditional and electronic commerce.

Nevertheless, because of the ways in which it differs from traditional commerce, electronic commerce raises some new and interesting technical and legal challenges. These include:

- Satisfying traditional legal requirements for reduction of agreements to signed documents;
- Applying legal rules of evidence to computer based information; and
- Interpreting, adapting and complying with many other existing legal standards in the context of electronic transactions.[30]

From a legal perspective, one of the most significant issues in electronic commerce is how to create enforceable electronic contracts for the sale of goods and services or how to ensure that a digital transaction will be at least as enforceable and valid as a traditional paper-based transaction. In every business environment, whether transactions are executed in person (face-to-face) or over distance, there are accepted customs and practices that determine, in conjunction with applicable legal rules, the parties rights and responsibilities.[31] These practices often include controls, such as:

---

[29] Subhajit Basu, Richard Jones "E-Commerce and The Law A Review of India's Information Technology Act, 2000" 12(1) *Contemporary South Asia* pp. 8-9(March, 2003).

[30] Diwan Sharma, *Electronic Commerce:A Managers Guide to E-Business* pp.218-219 (Vanity Books International,1st edn.,2000).

[31] *Ibid.*

- Signatures, to evidence agreements;
- Time and date-stamping, to provide proof of dispatch, submission, receipt or acceptance; and, in some cases;
- Witnesses, notaries or other trusted third parties, to acknowledge and authenticate transactions.

The purpose of this control is to create the necessary level of certainty in business transactions. Although electronic commerce is expanding rapidly, the development of corresponding legal and control infrastructure has lagged behind to create viable electronic equivalents to traditional Contracting activities. It is necessary to develop legal mechanisms or supportable legal analogs for the electronic commerce infrastructure. The goal of such mechanisms is to make electronic transactions at least as efficient, secure and legally binding as traditional commercial transactions, without forcing users to negotiate customized terms and conditions.[32]

1.3. Definition of E-Commerce

E-Commerce is the mode of conducting business through electronic means. However, there exists no standard definition for the term yet and different organizations have defined it diversely. E-Commerce means the production, distribution, marketing, sale or delivery of goods and services by electronic means.[33] E-Commerce is the application communication and information sharing technology among trading partners to the pursuit of business objectives. E-Commerce can be defined as modern business methodology that addresses the needs of the organization, merchants and consumers to cut costs while improving the quality of goods and services and speed of service delivery. E-Commerce is associated with the buying and selling of information, products, and services via computer networks. A key element of E-Commerce is information processing. E-Commerce is generally described as a method of buying and selling products and services electronically. The main vehicle of E-Commerce remains the internet and

[32] *Ibid.*

[33] Aashit Shah, Parveen Nagree, et. al., "Legal Issues in E-Commerce," *available at: http://*www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf (last visited on January 6, 2012).

the World Wide Web, but e-mail, fax and telephone orders is also used for conducting business.[34]

E-Commerce is a commerce based on bytes. E-Commerce is the commercial transaction of services in an electronic format. E-Commerce may also refer to the paperless exchange of business information using a suite of technologies such as Electronic Data Interchange (EDI) Electronic Mail (E-mail) Electronic Fund Transfer (EFT) Credit Cards, Fascimile (Fax) Electronic Bulletin Board Systems (EBBS) and Data Base Services. In simple terms, E-Commerce is a form of computerized buying and selling both by consumer and from by company, which facilitates choosing the goods, ordering. It is delivery after sales support and payment.[35] E-Commerce is not only about simple transactions of data but also general commercial acts such as publicity, advertisements, negotiations, contractors and fund settlements.[36] It refers to all forms of transactions relating to commercial activities, including both organizations and individuals that are based upon the processing and transmission of digitized data, including text, sound and visual images.[37]

The amount of trade conducted electronically has grown dramatically since the spread of the internet. A wide variety of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, internet marketing, online transaction processing, Electronic Data Interchange (EDI), automated inventory management systems, and automated data collection systems.[38]

Electronic Commerce comprises the electronic sale by online stores of downloadable soft merchandise such as music, e-books, e-newsletters, photos and video recordings, software and documents (direct E-Commerce), the electronic ordering of tangible products (indirect E-Commerce), online securities transactions as

---

[34] Mr Rajiv Rastogi"India Country Report on E-Commerce Initiatives", Director Department of information Technology, Ministry of Communication and Information Technology India" *available at*:*http://*www.unescap.orgtidpublicationpart_ three2261_ind.pdf (last visited on January 4, 2013).

[35] Tabrez Ahamad , *Cyber law E-Commerce and M-Commerce* p.2 (A.P.H. Publishing Corporation, 1st edn., 2003).

[36] Guidelines of E-Commerce, Ministry of International Trade and Industry (MITI), Japan (1996)., *available at*: *http://*www.kantei.go.jp/foreign/980817densi.html (last visited on June 3, 2012).

[37] While Paper on E-Commerce, OECD (1997)., *available at*:*http//:*www.oecd.org/ sti/2093249. pdf (last visited on June 7, 2012).

[38] Pradeep Kaur, Mukesh M Joshi "E-Commerce in India: A Review" 3(1) *International Journal of Computer Science and Technology* p.802 (January-March, 2012).

well as the provision of financial or other services. It also includes the subscription and use of an Internet Service Provider (ISP) or an Online Service Provider (OSP), and has been held to cover Electronic Data Interchange (EDI), Electronic Fund Transfers (EFT) and all credit and debit card activity.[39]

The World Trade Organization (WTO)[40] Ministerial Declaration on E-Commerce defines E-Commerce as the production, distribution, marketing, sales or delivery of goods and services by electronic means. The six main vehicle of E-Commerce that have been recognized by WTO are telephone, fax, TV, electronic payment and money transfer system, electronic data interchange (EDI) and the internet. According to European Commission,[41] E-Commerce encompasses more than the purchase of goods online. It includes a disparate set of loosely define behaviour, such as shopping, browsing the internet for goods and services, gathering information about items to purchase and completing the transaction. It also involves the fulfillment and delivery of those goods and services and inquiries about the status of orders. Like any other sustained business activity is also means conducting consumer satisfaction surveys, capturing information about consumers and maintaining consumer databases for marketing promotions and other related activities.

The Gartner Group[42] defines E-Commerce as an evolving set as:

(a) Home-grown or packaged software applications, which links multiple enterprises or individual consumers to enterprises for conducting business.

(b) Business strategies aimed at optimizing relationship among enterprises and between individuals and enterprises with information technologies.

(c) Business process (such as procurement or selling or order status checking or payment) that, by definition, cross boundaries and

(d) Technologies and tools that enable these applications, strategies and process to be implemented and realized.

---

39 Parikshit Dasgupta Parikshit, "India: Defining Jurisdictions in E-Commerce Taxations: Application of Traditional International Taxation Principles to E-Commerce" *available at*:*http://*www.mondaq.comindiax22619income+taxdefining+jurisdictions+in+ecommerce+taxations (last visited on September18, 2011).

40 See, *available at*: *http://* www.wto.org. (last visited on September 18, 2011).

41 See, a*vailable at*: *http://*europa.eu.int. (last visited on September 18, 2011).

42 See, a*vailable at*: *http://* www.gartner.com.(last visited on October 16, 2013).

The electronic commerce is all about commercial transactions, whether between private individuals or commercial entities, which take place in or over electronic networks. The only important factor is that the commercial transactions take place over an electronic medium.[43]

The Organization for Economic Cooperation and Development (OECD) defines electronic commerce as a new way of conducting business, qualifying it as business occurring over networks, which use non-proprietary protocol that is established through an open standard setting process such as the internet.[44] The Asia Pacific Economic Co-operation (APEC) has adopted a wider definition of E-Commerce to include all business activity conducted using a combination of electronic communications and information processing technology.[45]

The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) has also defined E-Commerce as the process of using electronic methods and procedures to conduct all forms of business activity.[46]

The Ministry of Economic Affairs of the Netherlands defined E-Commerce as all business transactions that are carried out electronically with a view to improving the efficiency and effectiveness of market and business processes.[47]

Kalakota and Whinston[48] define electronic commerce as a modern business methodology that addresses the needs of organizations, merchants and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery. The term also applies to the use of computer network to search and retrieve information in support of human and corporate decision-making. These authors further add that E-Commerce involves the buying and selling of information,

---

43 L. J. Davies, "A Model for Internet Regulation" (1998)., *available at: http://* www.scl.org. /content/commerce (last visited on October12, 2013).

44 Didar Singh," Electronic Commerce Issues of Policy and Strategy for India" (September, 2002). *available at*: *http://* www.icrier.orgpdfwp-86.pdf (last visited on October 11, 2013).

45 Aashit Shah, Parveen Nagree, et.al., "Legal Issues In E-Commerce" *available at*: *http://* www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf (last visited on November 8, 2010).

46 *Ibid.*

47 Norel Rosner, "Features - International Jurisdiction in European Union E-Commerce Contracts," *available at*: *http://*www.llrx.com/features/eu_ecom.htm (last visited on November 8, 2010).

48 Diwan Sharma, *Electronic Commerce: A Managers Guide to E-Commerce* pp.77-78 (Publication Vanity Books International,1st edn.,2000) .

products and services via computer networks today and in the future via anyone of the myriad of network that makes up the Information Superhighway.

Kestenbaum and Straight provides another description of Electronic Commerce as Electronic Commerce is the integration of e-mail, electronic funds transfer, Electronic Data Interchange and similar techniques into a comprehensive electronic-based system of business functions. The Buyer's Guide to Electronic Commerce gives yet another definition as Electronic commerce is using information technology to improve relationships between business partners. In spite of the fact that the literatures provide various definitions of Electronic Commerce, several features of Electronic Commerce that are common to all definitions stand out. First, organizations use Electronic Commerce to simplify and streamline business processes by substituting electronic means for paper documents. The most prevalent and well-known applications of Electronic Commerce are Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT), Electronic Mail (e-mail) and the World Wide Web (WWW).These technologies accrue many benefits to organizations. One such benefit involves transforming document based business processes such as simple order processing into a complete supply chain management. This can be accomplished both for inter and intra organizational transactions.[49] Second, Electronic Commerce enables and facilitates the formation of electronic markets. Bakos[50] defines an electronic market as an interorganisational system that allows the participating buyer and seller to exchange information about prices and product offerings. Klein and Langenohl to include electronic shopping systems have revised this definition. They state that electronic market involves as the totality of exchange relationship between market participants with potentially the same rights.

Kalakota and Whinston[51] articulate a classification scheme for activities that can be accomplished using Electronic Commerce.

- Transactions between a company and consumer over public network for the purpose of home shopping or home banking;
- Transactions with trading partners using EDI;
- Transactions for information gathering such as market research;

[49] *Ibid.*
[50] *Ibid.*
[51] *Ibid.*

- Transactions for information distribution includes advertising, sales and marketing.

From the aforementioned definitions, hence, it may infer as follows that Firstly, E-Commerce presupposes the existence of a business transaction. Secondly, the parties to such a transaction will maintain contact through electronic means rather than conventional ways of communication. Lastly, E-Commerce is designed to create a more efficient business environment.

1.4. E-Commerce: A Categorization

There are several categories of E-Commerce being used now days. These categories are classified based on the nature of the transactions, including Business-to-Consumer (B2C), Business-to Business (B2B), Consumer-to-Consumer (C2C), Consumer-to-Business (C2B), and No Business and Government, and Organizational (Intrabusiness). As an interested party can use various methods to participate in Electronic Commerce. Electronic Commerce could be further classified into different types based on different classifying standards as follows.

1.4.1. Business-to-Business (B2B)

This model defines that Buyer and Seller are two different entities. It is quite similar to manufacturer issuing goods to the retailer or wholesaler.[52] Business-to-Business refers to the full spectrum of E-Commerce that can occur between two organizations. Among other activities, Business-to-Business (B2B) E-Commerce includes purchasing and procurement, supplier management, inventory management, channel management, sales activities, payment management, and service and support.[53] While we may be familiar with a few Business-to-Business (B2B) pioneers e.g., Chemdex (www.chemdex.com), Fastparts (www.fastparts.com), and FreeMarkets (www.freemarkets.com) some other exciting new consortia are emerging. Business-to-Business E-Commerce has been undertaken solely via

[52] S.Sai Sushanth, "E-Commerce and Law:Trends and Challenges" 3(2) *UACEE International Journal of Advances in Computer Science and its Applications* p.57(2013).

[53] S. Sudalaimuthu, J Lilly, Emerging Trend of E-Commerce in India, available *on http://*www.fibre2fashion.comindustry-articlemarket-research-industry-reportsemerging-trend-of-E-Commerce-in-indiaemerging-trend-of-E-Commerce-in-india1.asp (last visited on October 12, 2013).

proprietary network and is usually referred to as Electronic Data Interchange (hereinafter referred to as EDI).

Open network, particularly the internet is increasingly becoming the communications medium of choice for business. EDI is nothing more than a technology for exchanging information. One computer is linked to another and a stream of data is sent across the link. At this level, the only distinction from a fax message is that the recipient can easily edit his copy. While EDI becomes interesting, both commercially and legally, the messages are structured in such a way that they can be processed automatically.[54] The question that arises for consideration in case of an EDI transaction is the extent to which the conditions of the network provider are binding on each individual user of the network the answer appears to lie in the judgment of the English court in *Clarke* v. *dunraven.*[55] The court held that if various people enter into agreement with the same person and all of them are using his services, then the contract is also binding among the individual persons *inter se.*

1.4.2. Business-To-Consumer (B2C)

The basic concept of this model is to sell the product online to the consumers.[56] Business-to-Consumer E-Commerce refers to exchanges between businesses and consumers, e.g., Amazon.com, Yahoo.com and Schwab.com. Similar transactions that occur in business-to business E-Commerce also take place in the Business-to-Consumer context. These include sales activities, consumer search, frequently asked questions, service, and support.[57]The commercial world fundamentally changed only after the introduction of the World Wide Web, or open networks. At present, a large part of the profits from electronic commerce goes to Business-to-Business (B2B). However, consumer transactions are in the process of rapid development and should mean big business in the near future. This business should take several forms, such as

---

[54] R.K.Chaubey, *An Introduction to Cyber Crime and Law* pp.793-794(Kamal Law House, Kolkata, 1st edn., 2008).

[55] (1897) AC 59.

[56] S.Sai Sushanth, "E-Commerce and Law: Trends and Challenges" 3(2) *UACEE International Journal of Advances in Computer Science and its Applications* p.57(2013).

[57] S. Sudalaimuthu, J Lilly, "Emerging Trend of E-Commerce in India", *available at http:*//www.fibre2fashion.comindustry-articlemarket-research-industry-reportsemerging-trend-of-e-ommerce-in- indiaemerging-trend-of-E-Commerce-in-india1.asp (last visited on October12, 2013).

electronic shopping, customer support, and product delivery and the volume of transactions should multiply.[58]

In general, where two or more commercial entities enter into agreements then they can usually agree to whatever terms they so wish. The position can differ considerably with other types of contract, as in business to Consumer E-Commerce where one of the parties acts as a consumer. Consumer protection legislation in various countries often imposes limits on the terms and conditions that may be excluded or varied and these cannot be overridden by agreement. The terms which attempts to avoid the legislative provisions are automatically void. Consumer regulation is an all-pervasive topic, which has several aims. Contrary to many views, commercial concerns often welcome some degree of consumer protection. Not only does it give consumers the confidence to interact and enter into commercial transactions with the commercial entities, but it also informs the commercial entities of what they can do and how they can act. The general perception of E-Commerce among consumers is that it poses a greater degree of risk than other more standard forms of commerce. Measures for consumer protection could help to allay these fears and encourage the take up of E-Commerce. This would bring benefits to all actors in the activity, to the economic development of the jurisdiction, to the economic activity of the commercial entities, and to a greater degree of freedom of choice for the consumer.[59]

1.4.3. Consumer-To-Consumer (C2C)

The Consumer-to-Consumer exchanges involve transactions between and among consumers. These exchanges may or may not include third party involvement as in the case of the auction-exchange e-Bay.[60] The Consumer-to-Consumer (C2C) category involves business transactions among individuals using the internet and web technologies. Using Consumer-to-Consumer (C2C), consumers sell directly to other consumers. For example, through classified ads or by advertising, individuals sell

---

58 Yun Zhao, *Dispute Resolution in Electronic Commerce* p.24 (Brill Academic Publishers, The Netherlands, 2005).

59 R.K. Chaubey, *An Introduction to Cyber Crime and Law* p.795 (Kamal Law House, Kolkata, 1st edn., 2008).

60 S. Sudalaimuthu, J Lilly, "Emerging Trend of E-Commerce in India", *available at: http://*www.fibre2fashion.comindustry-articlemarket-research-industry-reportsemerging-trend-of-E-Commerce-in-indiaemerging-trend-of-E-Commerce-in-india1.asp(last visited on October 12, 2013).

services or products on the Web or through auction sites such as ubid.com. E-Bay.com is a good example of a Consumer-to-Consumer (C2C) E-Commerce company. Using this web site, consumers are able to sell a wide variety of products to each other. Consumers are also able to advertise their products and services in organizational intranets and sell them to other employees.[61] Other activities include classified ads (e.g.,www.numberoneclassifieds.com), games (www.heat.net), jobs (www.monster.com), Web-based communication (www.icq.com), and personal services (e.g., Yahoo Personals, webpersonals.com).[62]

1.4.4. Consumer-To-Business (C2B)

The Consumer-to-Business (C2B) E-Commerce involves individuals selling to businesses. This may include a service or product that a consumer is willing to sell. In other cases, an individual may seek sellers of a product and service. Companies such as priceline.com, travelbid.com, and mobshop.com for travel arrangements are examples of C2B. Individuals offer certain prices for specific products and services.[63] Consumers can band together to form and present themselves as a buyer group to businesses in a Consumer-to-Business relationship. These groups may be economically motivated as with the demand aggregator, Mercata.com, or socially oriented as with cause-related advocacy at voxcap.com.[64]

1.4.5. Nonbusiness and Government

The E-Commerce applications in government and many non-business organizations are on the rise. Several government agencies in the United States have been using E-Commerce applications for several years, including the Department of Defense, Internal Revenue Service, and the Department of Treasury. Universities are using E-Commerce applications extensively for delivering their educational products and services on a global scale. Not-for-profit, political, and social organizations also use E-Commerce applications for various activities, such as fundraising and political

---

61 Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p. 52 (Academics, California, 2002).

62 *Ibid.*

63 Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.52 (Academics, California, 2002).

64 S. Sudalaimuthu, J Lilly, "Emerging Trend of E-Commerce in India", *available at http://*www.fibre2fashion.comindustry-articlemarket-research-industryreportsemerging -trend-of-E-Commer ce -in-indiaemerging-trend-of-E-Commerce-in-india1.asp (last visited on October 12, 2013).

forums. These organizations also use E-Commerce for purchasing (to reduce cost and improve speed) and for customer service.[65]

1.4.6. Organizational (Intrabusiness)

Organizational or intrabusiness E-Commerce involves all the E-Commerce related activities that take place within the organization. The organization intranets provide the right platform for these activities. These activities may include exchange of goods, services, or information among the employees of an organization. This may include selling organization products and services to the employees, conducting training programs, offering human resources services, and much more. Although, they are not direct selling and buying, some of these activities provide support for a successful E-Commerce program in human resources management, finance, and marketing.[66]

1.5. E-Commerce: A legal Mechanism

The E-Commerce refers buying and selling goods and services through electronic means specially on the internet but E-Commerce cannot be flourished without vibrant legal mechanism. The vital role is played in the E-Commerce mechanism as following.

1.5.1. Regulation of Digital Signature and Transaction under Information Technology Act, 2000

Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) was passed to fulfill the following three objects:

- To respond and give the effect to the United Nations Cell to all states to consider Model Law.
- To provide legal recognition for transactions carried out by means of electronic data interchange.
- To facilitate electronic filing of documents with the government agencies so as to promote efficient delivery of government services.[67]

---

65 Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.52 (Academics, California, 2002).

66 *Id.* at p.56.

67 Farooq Ahmad, *Cyber Law in India* p.32 (New Era Publication, Delhi, 4th edn., 2013).

Apart from the above stated objectives, the principal propellant on which the whole structure of the Act is based that is trust reposed between business partners. The breach of trust must be subject to law. The users of information technology must have trust in the security of information and communication infrastructure. The IT Act, 2000 was passed to facilitate electronic commerce and hence it provides legal recognition to electronic records, to digital signature etc. Main electronic transactions under the Act are:

1.5.1.1. Asymmetric Cryptostem

The word Cryptology Stems from Greek root meaning 'hidden word' and is used to describe the ancient science of secret communications. It means a system capable of generating a secure key pair consisting of a private key and public key.[68] This definition pertains to the dual key encryption techniques. Encryption is a technique to convert data into an unintelligible form that cannot be recovered into the original format without a secret decryption key. The object of applying cryptography to documents to transfer over the open networks, such as the internet, is to prevent vital information getting into the hands of unauthorized persons.[69]

There are basically two types of encryptions

- Symmetric(secret/private)key
- Asymmetric (public) key

Private or Symmetric key creates digital signature and public key verifies the digital signature which is called dual key encryption techniques.[70]This cryptographic technique involves the use of two cryptographic keys -a public key and a private key. The public key is freely distributed and made available to anyone who wishes to send a message to a given person. Any message that is sent to such person in confidence is encrypted using this public key and, since messages, encrypted using this public key can only be deciphered with the corresponding private key. The sender of the message can be sure that the message would reach the intended recipient. The encryption used

[68] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.635 (Universal Law Publication Co.2nd edn., 2000).
[69] *Ibid.*
[70] Tabrez Ahamad, *Cyber Law E-Commerce and M-Commerce* p.77 (A.P.H. Publishing Corporation, 1st edn.,2003).

for these keys is of such a high degree of complexity that it is theoretically impossible to crack within a reasonable timeframe.[71]

Transaction security is a significant barrier to the development of E-Commerce. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. The most reliable means is through cryptography (i.e. encryption and decryption techniques). Cryptography uses sophisticated mathematical algorithms, particularly a technology known as 'Asymmetric Cryptography'. Cryptography can be differentiated between the following:

- Use of cryptography for confidentiality of a message; and
- Use of cryptography in digital signature.

The most popular and useful method of encryption for general messaging is public key cryptography that is encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys, both of which are mathematically linked. One key is used for encryption and the other corresponding key is used for decryption. Each user has a pair of keys, of which the private key is kept secret and the public key is open to all.[72]

1.5.1.2. Adoption of Digital Signature

The term digital signature is defined in section 2(p) of Information Technology Act, 2000 as "Digital Signature" means authentication of an electronic record by a subscriber by means of an electronic method or procedure in accordance with a provision of section 3[73] of Information Technology Act, 2000. This definition is taken from the Singapore Electronic Transactions Act, 1998 and indicates the method commonly used in the West to verify electronic documents. "Digital Signature" means a Signature affixed in electronic from consisting of a transformation of an electronic record using asymmetric cryptosystem and a hash

---

71 Rahul Malthan, *Law Relating to Computers and Internet* p.172 (Butterworths India, New Delhi,1st edn.,2000).

72 Subhajit Basu, Richard Jones," E-Commerce and The Law: A Review of India's Information Technology Act, 2000"12(1) *Contemporary South Asia* pp.7-24 (2003).

73 See, Section 3 of The Information Technology Act, 2000 as (1) Subject to the provisions of this section any subscriber may, authenticate ail electronic record by affixing his digital signature. (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function, which envelop and transform the initial electronic record into another electronic record.

function[74] such that a person having the initial untransformed electronic record and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made. The term hash function is defined by way of Explanation to section 3(2) of the Information Technology Act, 2000.[75]

It led to the acceptance of cryptography, a data encryption technique, which provided just that kind of message protection. Based on the nature and number of keys cryptography has evolved into Symmetric (private key cryptographic system) and Asymmetric (public key cryptographic system) cryptography. In symmetric cryptography a single secret key is used for both encryption and decryption of a message, whereas in asymmetric cryptography encryption and decryption is done involving an asymmetric key pair consisting of a public and a private key. A digital signature involves two components-the public key and the private key. The sender signs a document using his private key that ensures the document's safety in transit as the text is encrypted and only the sender has access to his private key.[76]

Therefore, by signing a document with it, he authenticates that it has originated with him and not been tampered with enroute. The recipient of this document uses the sender's public key to authenticate the encrypted document and to decrypt it into a readable text format. Under Section 21 of The Information Technology Act, 2000, Certification Authority (hereinafter referred to as CA) issues certificates and stands responsible for them. The CA signs these certificates. This enables users to know which CA created each certificate. The signature also ensures

---

[74] "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible;
(a) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) That two electronic records can produce the same hash result using the algorithm. See, R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1000 (Kamal Law House, Kolkata, 1st edn., 2008).

[75] See, Sec.3(2) of The Information Technology Act,2000, The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

[76] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.782 (Kamal Law House, Kolkata, 1st edn., 2008).

that a third party has not altered or corrupted the certificate at any point of time. In India, the Indian IT Act, 2000 authorizes the Controller of Certifying Authorities (hereinafter referred to as CCA) to license and regulate the working of CAs, who issue digital signature certificates for electronic authentication of users.[77]

A digital Signature can be used as a verification tool by any person who has got access to the user's public key. It provides a convenient method for the receiver of the message to verify and satisfy himself that the message did in fact come from the person who affixed the digital Signature to the message. Since the Signature uses the original text as an input to the encryption algorithm, the Signature will not decrypt properly, if the message is altered in even the slightest way. Thus, the person receiving the message can be sure that the message has been received without any alternation and that the Signature is not copied from a different message. Digital Signature generally contains 1024 bites. Therefore, it has a very long life.[78]

Since the signature uses the original text as an input to the encryption algorithm, the signature will not decrypt properly if the message is altered in even the slightest way. As a result, the recipient can be sure that the message has been received unaltered and that the signature has not been copied from a different message. The reasons for placing a digital signature on an electronic document are exactly the same as the reasons for placing a handwritten signature on a paper document.[79]

They are:

- **Identification:** By placing a signature on a document, the signer identifies himself by the unique style of writing his name. Similarly, a digital signature uniquely identifies the sender of an electronic message.
- **Authentication:** By performing the act of signing, the signer acknowledges that he authorizes and adopts the contents of the document. Similar, intent can be attributed to the sender of the digitally signed e-mail message.
- **Security:** A signature on a document should be difficult to forge. Moreover, some aspect of the signature, such as the individuality of the style of the person signing,

---

77 *Ibid.*
78 *Ibid.*
79 *Ibid.*

offers security to the other party that as to the identity of the signer. Digital signatures offer the same form of security.

- **Tamper resistance:** The nature of a written signature is such that changes to the signed text or the signature itself are clearly apparent except in the case of the cleverest forgeries. A digital signature, if anything, is even more tampering proof as they are almost incapable of being forged without actually altering the message irretrievably.

1.5.1.2.1. Digital Signature and Public Key Infrastructure Process

The basic problem with the aforesaid digital signature regime is that it operates in online and software driven space without human intervention. Sender sends a digitally signed message then recipient receives and verifies it. The only requirement is that both sender and the recipient to have digital signature software at their respective ends. A digital signature certificate security bind the identity of the subscriber. It contains name of the subscriber, his public key information, name of the certifying authority who issued the digital signature certificate, its public key information and the certificate's validity period. These certificates are stored in an online repository that is publicly accessible repository maintained by the Controller of Certifying Authorities or in the repository maintained by the Certifying Authority. Every Certifying Authority (CA) has to maintain operation as per its certification practice statement (CPS). The Certification Practice Statement (hereinafter referred to as CPS) specifics the practices that each Certifying Authority employs in issuing digital signature certificates.[80]

The mass implementation of digital signature certificates in the internet environment is done via Public Key Infrastructure. It establishes a framework or system to use digital signature certificates, encryption and digital signatures as an authentication mechanism and devises management methods for such usage. The basic idea behind Public Key Infrastructure (hereinafter referred to as PKI) is to integrate the use of digital certificates, CAs and other security mechanisms to provide

---

[80] Vakul Sharma, *Information Technology Law and Practice* p.32 (Universal Law Publication Co., 1st edn., 2004).

an infrastructure that can be used to validate each party involved in E-Commerce, thereby making E-Commerce more secure.[81]

1.5.1.2.2. Public Key Infrastructure (PKI) Processes

Public Key Infrastructure (hereinafter referred to as PKI) is about the management and regulation of key pairs by allocating duties between contracting parties (Controller /Certifying Authority/ Subscribers), laying down the licensing and business norms for Certifying Authorities and establishing business processes or implications to construct contractual relationships in a digitized world.[82] The idea is to develop a sound public key infrastructure for an efficient allocation and verification of digital signatures certificates.

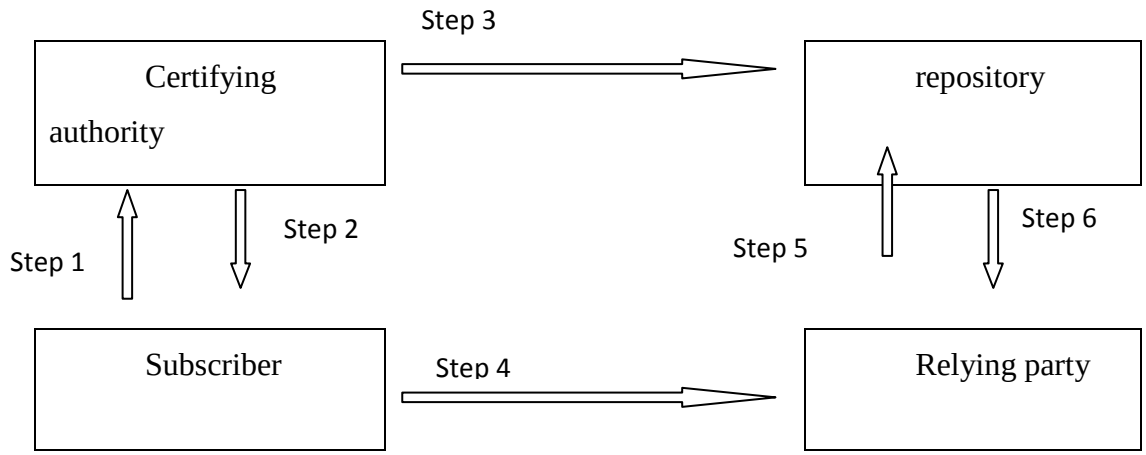


Figure 1.4: PKI process

Step l: Subscriber applies to Certifying Authority (CA) for Digital Signature Certificate.

Step 2: CA verifies identity of Subscriber and issues Digital Signature Certificate.

Step 3: CA forwards Digital Signature Certificate to Repository maintained by the Controller.

Step 4: Subscriber digitally signs electronic message with Private Key to ensure Sender Authenticity, Message Integrity and Non-Repudiation and sends to Relying Party.

---

81 *Ibid.*
82 *Ibid.*

Step 5: Relying Party receives message, verifies Digital Signature with Subscriber's Public Key, and goes to Repository to check status and validity of Subscriber's Certificate.

Step 6: Repository does the status check on Subscriber's Certificate and informs back to the Relying Party.

1.5.2. Regulation of Certifying Authority

The problem of identification of public key holder can be solved by appointing a third party, trusted by sender as well as recipient to perform the tasks necessary to associate a person or entity with a specific public key. This third party is generally called as Certifying Authority (hereinafter referred to as CA). It is a trusted body either public or private that ascertain the identity of the applicant of digital signature certificate and certifies that the public key of a public-private key pair used to create digital signature belongs to that person. The process of issuing a certificate differs from CA to CA. Generally, it requires:

a. Public-private key pair to be generated by the applicant.
b. Proof of identity such as identity card, driver's license or passport.
c. The applicant demonstrates that he/she holds the private key corresponding to the public key without disclosing the private key. Once the CA has verified the association between an identified person and a public key, the CA then issues a certificate. The person to whom the certificate is issued is called subscriber.[83]

Section 2(p) read with Section 3 of the IT Act, 2000 establishes that a signature could be sent using public key cryptography. In order to link the identity of the sender with the signature, it is necessary to attach a digital certificate, which is issued by so-called CAs that confirms the identity of the sender. The Information Technology Act, 2000 also lays down the duties of certification authorities, limitation of liabilities of certification authorities, and the framework for regulation of certification authorities that includes the appointment of a controller of certification authorities, and its powers. The regulation of CAs is primarily done by the Controller of Certification Authorities (Controller), who is vested with the functions of licensing, certifying, monitoring and overseeing the activities of CAs. The central government notified the Certifying Authority Rules (CA Rules) on 17 October 2000, which

[83] See, Sec. (2F) of The Information Technology Act, 2000.

prescribe the conditions under which CAs can apply for a license in India, and carry on their operations. The IT Act, 2000 has adopted an extremely complex mechanism for the registration and operation of the CAs.[84]

Section 19 of the IT Act, 2000 marks provisions for recognition of foreign certifying authorities for the purpose of this act. Some of the leading foreign certifying authorities are: VeriSign, Thawed, Global sign, Bel sign and Sure sign. British Telecom and Scotia Bank are also in this business. Section 30 of IT Act, 2000, provides every Certifying Authorities shall make use of hardware, software and procedures that are secured from intrusion and misuse. It provides a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions; adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and observe such other standards as may be specified by the regulations made by the controller. In this regard, controller should keep a computerized database in respect of all public keys for such Signature Certificates. He is expected to make those public keys to any person who applies for them to verify the digital signature. Controller will have powers to access any computer system, apparatus or records maintained by the Certifying Authorities.[85]

1.5.3. Digital Signature or electronic signature Certificate

In simple terms, a digital certificate is a reliable electronic method of signing electronic documents that provides the recipient with a way to verify the sender and also determine whether the content of the document has been tampered with digital certificates use a method of cryptography called asymmetric encryption. Unlike symmetric encryption, which uses the same secret password to view messages, asymmetric encryption, also called public key encryption, uses a pair of keys, namely a public and a private key. The public key is published in a public directory and the corresponding private key is kept secret.

So, the sender uses one key to encode the message and the receiver uses another matching key to decode the message. In a digital signature, the signer (say A) encodes the document with his own private key that is available only with him. The

---

[84] Subhajit Basu, Richard Jones, "E-Commerce and The Law: A Review of India's Information Technology Act, 2000"12(1) *Contemporary South Asia* pp.7-24 (2003).

[85] Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* p.80 (A.P.H. Publishing Corporation, 1st edn.,2003).

receiver decrypts the message with A's public key that is available publicly. Since the receiver is able to decode the message using A's public key, and since A is the only one who has access to his private key, everyone knows that the message is indeed signed by A. Further, the receiver cannot alter the data sent by A. This proves the authenticity of the document.[86]Section 35 in Chapter VII of IT Act, 2000 empowers Certifying Authorities to issue digital signature certificates. It empowers the Central Government to prescribe application fees to be paid by persons or getting a digital signature certificate. The Government has power to prescribe different fees for different classes of applicant before granting the digital signature certificate. The certifying authorities should satisfy himself that the applicant holds the private key corresponding to the public key to be listed in the digital signature certificate. The applicant holds a private key, which is capable of creating a digital signature and the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.[87]

Depending upon the level of inquiry, which a certifying authority may undertake to confirm the identity of public key holders, different types of certificates may be issued by the Certificate Authority (hereinafter referred to as CA). **Class I** certificates are designed for casual web browsing and secure e-mail and are issued to the individuals only. **Class II** are more expensive and confirm that the information provided by the subscriber in his/her application is in accord with the information available in a well recognized consumer data base. **Class III** certificates will require personal presence of the subject or he may submit registered credentials and pass an automated identification check. **Class IV** certificates involve through investigation of both an individual as well as organization whether private or public.[88]

1.5.4. Duties of Subscribers

The Chapter-VIII, the IT Act, 2000) contains sections 40 to 42. Every certifying authority has certain responsibilities. The subscribers too have certain responsibilities. Chapter- VIII specifies the duties of subscriber. The term "subscriber" is defined in section 2(2) (1) of the IT Act, 2000 as a person in whose name the digital signature certificate is issued. The IT Act, 2000 envisages a pair of

---

86 R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.785 (Kamal Law House, Kolkata, 1st edn., 2008).

87 *Id.*at p.81.

88 *Id.* at p.784.

keys - one private and the other public. It is the responsibility of the subscriber to retain control of his private key corresponding to the public key listed in its digital signature certificate. The subscriber should keep the identity of his digital signature secret. He should use the digital signature himself. He should not reveal it to others. He owes a duty to inform the certifying authorities without any delay in case his private key has been compromised in any manner. The Information Technology Draft Bill, 1998, Section 63(l) (g) included such fraudulent acts and makes it a crime. Such a clear definition is conspicuously absent in the IT Bill, 1999. The IT Act, 2000, has made amendments to section 464 of the Indian Penal Code, 1860 that comprehensively cover all kinds of fraudulent acts committed on or through the internet.[89]

1.5.5. E-Commerce Payment System

Over past twenty-five years, the world banking system has developed a number of different networks and services for the transfer of funds. Some of these, referred to as wholesale Electronic Funds Transfer (hereinafter referred to as EFT), are closed system which can only be used between regulated financial Institutions. The best known system is the Society for Worldwide Interbank Financial Telecommunications (hereinafter referred to as SWIFT). SWIFT is a co-operative organization under Belgian law, with headquarters in La Hulpe, near Brussels. SWIFT provides communications services to the international banking industry, payments and the member banks (approximately 1,600) including the central bank of most countries. The U.S. Federal Reserve is not a member, but participates in certain type of payments. Securities brokers and dealers, clearing and depository institutions, exchanges for securities, issues of traveler's cheques also participate in SWIFT. The profits from the global transfer of funds are vast. Consequently, SWIFT has had a turbulent life as its members have sought to gain advantages over each other by producing their own.[90]

Additionally, SWlFT has always been little more than a secure closed messaging operated under strict rules between banks. Under its rules, payment instruction sent by SWIFT are irrevocable guaranteed unconditional payments.

---

89 Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* p.83 (A.P.H. Publishing Corporation, 1st edn.,2003).

90 *Id.* at pp.65-66.

SWIFT has said that it is going to have interactive, query and response as well as store-and-forwarding file transfer and a new standards paradigm. In time, it says that it will also have to move to an Internet Protocol Infrastructure but the issues of security of migration to the new systems and how SWIFT intends running incompatible networks together remain unanswered. Since SWIFT pays for it developments out of the profits it earn from its funds transfer activities and these profits are already under serious attack from rival products and it may be the case that SWIFT does not have a future in the electronic commerce marketplace. Instead, its role will be taken over by some form of digital money.[91]

Markets of any sort involve transactions. These transactions usually end up in the seller being paid by the buyer. Until then, the whole transaction remains uncertain. The longer the delay in between undertaking to pay and actual payment, the greater is the uncertainty. The internet offers the prospect of a highly cost effective payment system for low value transactions. Technology is able to offer nearly instantaneous settlement of transactions. In order to achieve such an objective, security issue will need to be successfully addressed without losing all of the benefits that accrue from the internet's open structure.[92]

1.5.5. 1. Essential Features of Electronic Money

Money is a widely accepted medium of exchange, a store of value and a unit of account. It forms the basis of a smoothly functioning market system. With the advent of the internet and electronic commerce, we are in the process of shifting significantly from paper currency to electronic cash. Stored value cards with an embedded micro chip that stores money in digital form may become a customary circulating medium along with privately supplied digital cash is stored in computer hard drives.[93] This transaction from paper-based monetary system to an electronic payment system will reduce transactions costs, expand markets and empower individuals. The rules that govern the new monetary universe will have to be

---

[91] Tabrez Ahamad, *Cyber law E-Commerce and M-Commerce* pp.65-66(A.P.H. Publishing Corporation, 1st edn.,2003).

[92] Write B., Eggs in Basket, "Distributing the Risks of Electronic Signature" 6 *Computers and Law* p.30 (1995).

[93] James A.dorn, "The Future of Money in The Information Age", *available at*: *http://*www. cato.org/pubs/books/mpney(last visited on June 12, 2011).

transparent, equally applied and consistent. With individual freedom if people are to have trust and confidence in cyber- money and cyber-commerce.[94]

Another point which requires due attention is whether the electronic money is stored on a ledger maintained by third party or is stored on a token maintained by the consumer (token electronic money). There are many ways to implement an electronic token system. All these must passés some fundamental features.

(i) Monetary Value: Electronic tokens must have a monetary value. Electronic token without a monetary value are useless.

(ii) Exchangeability: Electronic tokens must be interoperable, that is, exchangeable as payment for other electronic tokens, paper cash, goods or services, lines of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfers and the like.

(iii) Irretrievability: Apart from exchangeability, electronic tokens must be able to be stored and retrieved.

(iv) Tamper-Resistance: Throughout their life cycle, electronic tokens should be difficult to tamper with copy or forge.[95]

1.5.5.2. Electronic Fund Transfer

The Electronic Fund Transfer (hereinafter referred to as EFT) is used for transferring money from one bank account directly to another without any paper money changing hands. EFT is the foundation of the cashless and checkless society where checks, stamps, envelopes, and paper bills are eliminated. The most popular application of EFT is the direct deposit option used by millions of workers in the United States. Instead of receiving a paycheck and depositing it into an account, the money is deposited to an account electronically. The Federal Reserve's Fed Wire and New York Clearing House Interbank Payment Systems (CHIPS) are two major users of EFT systems. Customers, Companies, and Government agencies use EFT for all kinds of applications. EFT is considered a safe, reliable, and convenient way to conduct business. Direct deposit is used for payroll, travel, and expense

---

[94] Jim Miller, "Answers to Frequently Asked Questions about Electronic Money or E-Money and Digiytal Cash," *available at: http*://www.ex.ac.ukRDavies/arian/ emoneyfaq.html (last visited on February 19, 2012).

[95] *Ibid.*

reimbursements, annuities and pensions, dividends, and government payments such as Social Security and veteran's benefits. Other types of EFT are frequently used for bill payments, retail purchases, internet purchases, corporate payments, and treasury management, and for the disbursement of food stamps and other government cash assistance. In broad terms EFT refers to any transfer of funds initiated through an electronic terminal, including credit card, ATM, Fed wire, and point-of-sale (POS) transactions. It is used for both credit transfers, such as payroll payments, and for debit transfers, such as mortgage payments. Many utility companies and sport clubs also use EFT.[96]

The advantages of Electronic Funds Transfer include the following:

- Reduced administrative costs
- Increased efficiency
- Simplified bookkeeping
- Enhanced security

At present, acceptance of this system has not been widespread. Banks process EFT transactions through the Automated Clearinghouse (hereinafter referred to as ACH) network. ACH is a secure network that connects all U.S. financial institutions. For electronic payments, funds are transferred electronically from one bank account to the billing company's bank, usually within 24 hours of the scheduled payment date. Another common application of EFT is for money transfer among banks and other financial institutions. When a customer pays for goods and services by cheques, the merchant collects these checks (assuming the checks are accepted) and sends them to its bank. The bank credits the merchant account and then sends these cheques to the clearing department. The clearing department separates the cheques by banks and transfers them to a clearinghouse. At this point, banks transfer cheques among themselves. The customer's bank eventually receives the cheque and debits the customer account. In some cases, these cheques are sent back to the customer, which marks the end of the process. If there are not sufficient funds in the customer's account, then the cheque is sent back to the merchant bank. The merchant must pay for the fee involved in the nonsufficient funds process and has to settle this with the customer or write it off as a bad cheque. The U.S. government monitors EFT

[96] Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.197 (Academic Press, California, 1st edn., 2002).

compliance through Regulation Electronic of the Federal Reserve Board, which implements the Electronic Funds Transfer Act (EFTA).[97]

The real revolution in funds transfer was started by bank to customer system known as retail EFT. These have been corporate cash management system (allowing business to give instructions to their banks either by the use of dedicated terminals or today using standard PCs over the internet) and consumer Electronic Funds Transfer Point of Sale System (hereinafter referred to as EFTPOS) which allow customer to make payments directly from their bank account to merchants. SWITCH is the main U.K. brand in this sphere. During the 1990s, national EFTPOS systems have become international through their Links to VISA and Master Card, Credit Cards to become universally payment mechanisms around the world. This has contributed to a change an international business practice driven not from the multinational doing business with each other but by tourists travelling and spending. The payment mechanisms developed for tourists are now being adapted for Electronic Commerce and may become serious alternatives to conventional bank to bank funds transfer.[98]

Bank to customer system known as retail Electronic Fund Transfer System (EFT) started revolution in transacting the funds. Data to this system has been made corporate cash management system and consumer Electronic Fund Transfer Point of Sale System (hereinafter referred to as EFTPOS) that allows customer to make payments directly from their bank account to merchants. During the 1990s, National Electronic Funds Transfer Point of Sale System (EFTPOS) has become international through their links to VISA and Master Cards. Now payment mechanism deployed for tourists is being adapted for electronic commerce. There mechanism may provide better alternatives to conventional bank to bank funds transfer.[99]

1.5.5.3. Secure Electronic Payment systems Infrastructure

In order to ensure the integrity and security of each electronic transaction, the Financial Service Markup Language (FSTC)'s e-check technology and other Electronic Payment System (EPS) utilize some or all of the following security measures. It should be noted that a number of these measures are used in other applications as well. For example, authentication is used for other security purposes,

---

97 *Id.* at p.198.
98 *Ibid.*
99 See, *available at*: *http:*//www.cybercash.com (last visited on February 12, 2014).

such as when logging in to a network, digital signatures is used for formal contracts.[100]

1.5.5.3.1. Digital Signatures

A digital signature is an electronic rather than a written signature that can be used by an individual to authenticate the identity of the sender of a message or of the signer of a document. The U.S. government now accepts these signatures and gives them the same rights and privileges as written signatures. This law was passed in June 2000. E-check technology also allows digital signatures to be applied to document blocks, rather than to the entire document. This allows part of a document to be separated from the original, without compromising the integrity of the digital signature. This technology would also be very useful for business contracts and other legal documents transferred over the Web.[101]

1.5.5.3.2. Authentication

Authentication is the process of verification of the authenticity of a person and a transaction. There are many tools available in the Electronic Payment Systems to confirm the authenticity of a user; for example, passwords and ID numbers are used to allow a user to log in to a particular site.[102]

1.5.5.3.3. Public Key Cryptography

Cryptography is the process of protecting the integrity and accuracy of information by converting (encrypting) data into an unreadable format, called Cipher Text. Only those who possess a private key can decipher (decrypt) the message into plain text. Public key cryptography uses two keys, one public and one private, to encrypt and decrypt data, respectively. Generally, a designated authority issues this public–private key combination. The cryptographic certificates used with an e-cheque enable a cheque payee to determine the validity of the signature. Public key cryptography uses a pair of keys, one private and one public. In comparison, private key cryptography uses only one key for encryption. The advantage of the dual-key technique is that it allows the businesses to give away their public key to anyone who

---

[100] Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.206 (Academic Press, California, 1st edn., 2002).

[101] *Ibid.*

[102] Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.206 (Academic Press, California,1st edn., 2002).

wants to send a message (sending a credit card number, for example). The sender can encrypt the message with the public key and send it to the intended businessperson over the internet or any other public network, the businessperson can then use the private key to decrypt the message. Naturally, the private key is not publicly known.[103]

1.5.5.3.4 Certificates

The Certificates provide a mechanism for establishing confidence in the relationship between a public key and the entity that owns the corresponding private key. A certificate can be thought of as similar to a driver's license. A driver's license is accepted by numerous organizations both public and private as a form of identification. Therefore, the driver's license can be accepted as a valid form of identification.[104]

1.5.5.3.5. Certificate Authorities

In the E-Commerce world, certificate authorities are the equivalent of passport offices in the government that issue digital certificates and validate the holder's identity and authority. Certificate authorities are similar to a notary public, a commonly trusted third party.[105]

1.5.5.4. Admissibility of Electronic Evidence

The United Nation Commission on International Trade Law (hereinafter referred to as UNCITRAL) Model Law of Electronic Commerce 1996 (Model Law) includes a provision dealing with admissibility and evidential weight of data messages. The expression data messages is defined to include information generated, sent, received or stored by electronic, optical or similar means, including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy. Article 9 of Electronic Commerce 1996 (Model Law), provides that the rules of evidence must not deny the admissibility of a data message in evidence on the sole ground that it is a data message, nor where the data message is the best evidence reasonably available, on the grounds that it is not in its original form. Specially,

---

[103] *Id.* at p.207.
[104] *Ibid.*
[105] Hossein Bidgoli, *Electronic Commerce: Principles and Practice* p.207 (Academic Press, California, 1st edn., 2002).

Article 9(2) Electronic Commerce 1996 (Model Law) states, information in the form of a data message shall be given due evidential weight. In a manner Reminiscent of Butera's case, the Model Law provides that in assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.[106]

Although the Model Law has been used as a template in more than 50 jurisdictions internationally, this particular provision was omitted from the Australian and New Zealand Electronic Transactions Acts, because it was thought that such a provision is best placed in a jurisdiction's evidence legislation and not in its electronic commerce legislation.[107]

The UNCITRAL Model law on Electronic Commerce (1996) deals with the admissibility and evidentiary weight of data messages in Article 9(1). The article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message because it is a data message (electronic format) or, if it is the best evidence that the person adducing it could reasonably be expected to obtain on the ground that it is not in its original form.[108] The Enactment Guide of the UNCITRAL Model Law on Electronic Commerce, as regards Art (9) states, the purpose of.... Art 9(1) is to establish that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form; puts emphasis on the general principles stated in Article 4 and is needed to make it expressly applicable to admissibility of evidence. Particularly complex issue might arrive in certain jurisdiction in an area.[109]

1.5.5.4.1. Types of Evidence

The Evidence is information that tends to prove or disprove a fact in question. Evidence may consist of documents including electronic document, public records, affidavits or the testimony of witnesses. It may also be an object, such as a murder

---

[106] Alan Davidson, *The Law of Electronic Commerce* pp. 305-306 (Cambridge University Press, New York, 1st edn., 2009).

[107] Alan Davidson, *The Law of Electronic Commerce* pp. 305-306 (Cambridge University Press, New York, 1st edn., 2009).

[108] See, Article 9(1)(a) of UNCITRAL Model Law on E-Commerce (1996).

[109] *Ibid.*

weapon, whose existence or appearance provides information about the fact in question. The law of evidence is a part of the law of procedure. The Indian Evidence Act applies to all judicial proceedings before any court. It does not apply to affidavits and proceedings before arbitrators.[110]

Almost all evidence to prove facts in litigation involving the internet will be computer generated. This is primarily because technology today only allows for internet usage through computers. Section 2(i) of the IT Act, defines a computer as any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic magnetic or optical impulse, includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

These are following three kinds of electronic document generated by computer.

1.5. 5.4.1.1. Real Evidence

It analyses which generated by the computer itself through the running of software and the receipt of information from other devices such as built-in clocks and remote sensors. This type of evidence is termed real evidence. Real evidence arises in many circumstances. If a bank computer automatically calculated the bank charges due from a customer based upon its tariff. The transactions on the account and the daily cleared credit balance. This calculation would be a piece of real evidence.[111]

1.5. 5.4.1.2. Hearsay Evidence

There are documents and records produced by the computer, which are copies of information supplied to the computer by human beings. This material is treated as hearsay evidence. Cheques drawn and paying-in-slips credited to a bank account are hearsay evidence.[112]The hearsay evidence is not admissible in the court of law in Indian law of evidence.

---

[110] *Ibid.*

[111] V.D. Dudeja, *Cyber Crimes and Law: Cyber Crimes and Law Enforcement* p.93 (Commonwealth, 1st edn.,2002).

[112] *Ibid.*

1.5. 5.4.1.3. Derived Evidence

The derived evidence is information, which combines real evidence with the information supplied to the computer by human beings to form a composites record. This too is treated as hearsay evidence in modern evidence statutes. An example of derived evidence is the figure in the daily balance column of a bank statement. Since, this derived from real evidence (automatically generated bank charges) and hearsay evidence (individual cheque and paying in entries).[113]

1.5. 5.4.2. Evidence and Computer Generated Evidence

The law should be indicative of positive acceptance of the use of information technology and dynamism to facilitate its growth. The proliferation of Computers/Internet has created a number of problems for the law. Many legal rules assume the existence of paper records, of signed records, of original records. The Law of Evidence traditionally relies on paper records as well though of course oral testimony and other kinds of physical objects have always been part of court-rooms, too. As more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities by available to demonstrate the legal rights that flow from them. The term reliability has caused confusion between the principles of authentication, best evidence, hearsay and weight. There has been a growing demand from industry and users for new types of signatures to effectively substitute the hand written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents. The advent of the internet is similar to that of the telephone, telegraph, and fax machine communication is facilitated. The internet must be facilitated the focus must be on facilitating the speed and use of technology with specific reference to evidence, the admissibility of electronic evidence in order to ensure a proper examination of electronic evidence adduced before the court. The system so devised to encompass technologies. Technologies have revolutionized our lives.[114]

With the enactment of the Information Technology Act, 2000, the law recognizes electronic counter parts of paper documents and signatures. They are admissible in courts. They may be proved with few barriers such as requirements of

---

[113] *Ibid.*

[114] V.D. Dudeja, *Cyber Crimes and Law: Cyber Crimes and Law Enforcement* p.93 (Commonwealth, 1st edn.,2002).

originals. Thus, electronic records are vulnerable to tampering and there is no full proof way of authentication. However, the acceptance and reliance on such forms of evidence to be tailored to the needs of each case Hon'ble Judges may exercise careful method of deciding this as there is no objective standard for integrity depending on the peculiarity of the system.[115]

1.5. 5.4.3. Indian Position

The Indian Evidence Act, 1872 when compared with the General Clauses Act, 1897, excludes the world 'written' from the definition of 'document'. The focus of this statute is the purpose the document is to be used for i.e; recording the matter. The Evidence Act further goes on that, some limited exception, when the contents of a document are to be proved, the document itself has to be adduced and copies of it shall not be admissible.[116] The way to examine an electronic document is by displaying it on a secondary device, either a screen or a printout. It is a tenable argument that such display is not original, but amounts to a copy and is therefore, inadmissible as evidence. Indian law does not resolve this issue. An alternative route could be using the evidence for corroborative purposes. Oral evidence can be introduced if it relates to the relevant fact.[117]

Further, under the second proviso to section 60 of the Indian Evidence Act, if the oral evidence refers to the existence or condition of any material thing other than a document, the court may require the production of such material thing for inspection. Thus, if oral evidence as to the existence of a contract is adduced, then computer evidence may become admissible as it can be termed as material thing. Therefore, computer evidence may be allowed to corroborate the oral evidence.

In *MP Verma* v. *Surinder Kaur,*[118] Indian courts have allowed tape recordings to be admissible in this manner. With the passing of Information Technology Act, 2000 discussion on this point becomes purely academic. The Act through its amending section brings in a new section 65B into the Indian Evidence Act which starts with the heading Admissibility of Electronic records. It says that any information contained in an electronic record with is pointed on a paper, stored,

---

[115] *Ibid*.
[116] See, Sec.64 of The Indian Evidence Act, 1872.
[117] See, Sec. 59 of The Indian Evidence Act, 1872.
[118] AIR 1982 SC 1043.

recorded or copied in optical or magnetic media produced by a computer shall be deemed to be also document, if the condition mentioned in this section are satisfied. Thus, with the amendment to the Evidence Law, an electronic document can for all practical purposes have the same legal effect as a paper based original document so long as the conditions mentioned in sub clauses of the amended section are satisfied.

1.6 Benefits of E-Commerce

E-Commerce leads to a win-to-win situation for both companies and customer. The companies can reach more customers all over the world, gather better information about them, target them more effectively and serve them better. The companies can also reduce cost considerably by reducing cycle time, sale and marketing cost, document processing costs and thus, able to improve working capital and productivity. The market places also create value for the third party intermediaries, which can earn transaction commissions and fees for value added services such as information capture and analysis, order and payment processing, integration of buying and seller's Information Technology system and consultancy services. However, the best rewards go to customer. They are able to compare products and prices easily, demand better quality of service at lower cost and in turn will compel suppliers to compete more fiercely than ever.[119]

There is a growing awareness among the business community in India about the opportunities offered by E-Commerce. Ease of internet access and navigation are the critical factors that will result in rapid adoption of Electronic commerce. Safe and secure payment modes are crucial too along with the need to invent and popularize innovations such as Mobile Commerce. India Reports provides accurate and easy to understand India specific reports that capture trends, map business landscapes and custom-made reports for specific needs. The other reports available on India Reports are on retail, outsourcing, tourism, food and other emerging sectors in India.[120]

V-Sates, E-Mail, Voice Mail Local Area Network (LAN) and Wide Area Network (WAN) have already been introduced. Instead of sending reports, management has access to information and data by merely pressing a button. Proctor

[119] Subhashis Data, "E-Commerce: An Overview in The Indian Context" 31(7-12) *Charted* Secretary p.1547 (2001).

[120] Shweta Sharma, Sugandha Mittal, "Prospects of E-Commerce in India," *available at:http://*www. rimtengg.comiscetproceedingspdfsadv_nw_tech43.pdf(last visited on June 4, 2012).

and Gamble has a 24-hour help desk which enables the company's local and global network away all the time. Communication is easier and more formal. There is no emphasis on hierarchy and work proceeds faster. The internet is a worldwide network of computers. Today, it spans 150 countries and has 40 million users. The internet provides unrivalled global reach useful to companies to expand operation overseas on a tight budget and as advertising medium and to download information. Laptop computers (portable personal computers) are creeping into executive life. Many companies have provided them to their top executive. It also enables a wide range of office work to be undertaken anywhere. It can store addresses, telephone numbers and other data. It enables one to keep in touch with head quarters and is very helpful in making presentation. Microsoft is said to be working on a wallet Personal Computer (PC). Wide Area Network (WAN) enables faster access to and preparation of data. An electrical giant with twelve manufacturing location uses information technology to coordinate the activities of all its Indian locations and integrate them with those of the parent company's worldwide operations. Quotations to customers are given within 48 hours whereas it took previously 20 days.[121] E-Commerce is growing in importance and means unprecedented opportunities for everyone. When a business takes advantage of the power of E-Commerce, it will be able to:

1.6.1. Increase customer satisfaction

The internet is always open, even on holiday; business is thus always open, 24 hours a day, 7 days a week and 365 days a year. Customers will appreciate the extra access to product updates, shipping details, billing information and more. since the internet knows no boundaries, customers can shop from home, work, or anywhere they can make a connection by connecting the E-Commerce and shipping systems, it would be possible to ship products faster and for less money.[122]

1.6.2. Increase sales volumes

The internet is a new channel to reach new customers. With a Web site, a company can automatically become a global provider of goods and services, with an edge over even the largest competitors. Interactive selling is advantageous because a

---

[121] Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* pp.7-8 (A.P.H. Publishing Corporation, 1st edn.,.2003).

[122] *Ibid.*

company is no longer limited by shelf-space or inventory concerns but instead offer all products to suit the customers' exact specifications.[123]

1.6.3. Decrease costs of doing business

E-Commerce helps cut out or streamline processes that eat away profits. For instance, exchange of information from advertising to availability updates can add to the cost of a sale. However, the web site can be an efficient, cost-effective communication vehicle customers can find timely, accurate information in one place when they need it. By using E-Commerce, everything from purchase orders to funds transfer can be handled faster and more efficiently. Even payment processing and bookkeeping are easier.[124]

- Easy reach to a fast growing online community
- Unlimited shelf place for products and services
- Fuse the global geographical and time zone boundaries
- Helps reach national and global markets at low operating costs.

1.7. Intellectual Property Right and E-Commerce

The World Intellectual Property Organization (hereinafter referred to as WIPO) is a specialized agency of the United Nations that works for the protection of legal rights in artistic and literary works, inventions, trademarks, and other original creations. Such rights are known as Intellectual Property Rights. The organization works for the promotion of international agreements on Copyrights, Patents, Trademarks, and other original creations. It also provided technological information and other assistance to developing countries. WIPO has a membership of more than 120 countries. It is situated in Geneva, Switzerland and WIPO administers two treaties. One product copyrights, the other products patents, trademarks and other original creations. Administrative agencies of the two treaties joined in 1983 and were replaced by that of WIPO when it was founded in 1967.

The agency became part of the UN in 1974. WIPO plays a particularly important role in educating Intellectual Property official worldwide about the importance of establishing and implementing strong Intellectual Property Rights and laws. On the one hand, The International Convention relating to Copyright called the

[123] *Ibid.*
[124] *Ibid.*

Berne Convention for the Protection of Literary and Artistic Works of 1886. The 14 countries adopted and agreed certain standard rules for the protection of literary and artistic works and agreed to protect works published in each of the member countries. On the other hand, Sound recordings are subject to the provisions of 1971 Geneva Convention for the Protection of Producers of Phonograms against unauthorized duplication of their Phonograms. Over 40 member countries, including the United Kingdom and the United States have adopted this convention. WIPO organized a conference in December 1996, inviting around 160 member countries, the agenda being modification of the existing norms and creation of new norms on Intellectual Property Rights, but with the new developments:

- Copyright of Electronic Records,
- Protection of Performers and Producers of Phonograms, and
- New form of Sui-generis (of one's own origin) Protection of Databases.

1.7. 1. Internet and Intellectual Property Right

First consideration that any company intends to commence E-Commerce activities should bear in mind about the protection of its intellectual assets. The internet is a boundless and unregulated medium and therefore the protection of Intellectual Property Rights (hereinafter referred to as IPRs) is a challenge and a growing concern amongst most e-businesses. While there are existing laws in India that protect IPRs in the physical world, the efficacy of these laws to safeguard these rights in E-Commerce is uncertain.[125] The computer's ability to share data with other computers over a network linked through telephone has led to a major telecommunication revolution. A computer network is a network consisting of a central computer (server) and a number of remote stations that report to it. Networking has led to the concept of Cyber space. Cybernetics is the comparative study of automatic communication and control in functions of living bodies and in mechanical electronic systems such as computers. The word cyber has evolved to denote a virtual space or memory. A cyber is analogous to human memory. It denotes the medium in which certain activities take place, like the way thoughts work in human memory. Activities take place in the back end of a computer and the results are

[125] Nishith Desai Associates, "Legal Issues in E-Commerce," *available at*: *http//*:www. nishithdesai.comResearch-PapersLegal_issues_ecom.pdf (last visited on February15, 2013).

displayed in the monitor. The data/documents stored in the electronic form as softcopies, which could be retrieved at any point of time and visualized in the monitor. Electronic Data consists of text, images voice and programmes. The present day data transmission is far superior in terms of speed, quality, visuals, utility, impact and convenience. The popularity of the internet raised critical questions regarding to regulations and governance, restrictions on the use of the internet could hamper its growth. The internet is global in nature. It is a fact that the growth and spread of the internet has become an important yardstick for measuring the growth and strength of any economy.[126]

E-Commerce entails the buying and selling of products and services at a distance. It is, therefore, becoming increasingly important to rely on the reputation attached to trademarks and other distinctive signs. Several addresses containing the trademark names of established companies have been registered as domain names, thus leading to disputes over their usage, as well as to allegations which are referred to as cyber-squatting. This practice has become so popular that it is estimated that 98 per cent of the words in Webster's English Dictionary at present have been registered as domain names. Selling innovative and interesting names as internet addresses is one thing, but cyber-kidnapping trademarks of existing businesses is another thing. The World Intellectual Property Organization (WIPO) has last year issued a report on the issue of trademarks and domain names, recommending practices and guidelines intended to prevent disputes in this area. They also accept complaints in this area and issue judgments from Geneva on the same. This process is, however, rather cumbersome and very expensive for poor countries and their firms.[127] The protection of IPRs requires that governments and the private sector develop and implement an appropriate mix of regulatory, contractual, and technological measures, and ensure adequate public awareness of the role of copyright and related rights in the information society. This would, on the one hand, provide protection to local industries in global markets and, on the other hand, investment and growth by providing a safe and legal environment.

---

[126] V.D.Dudeja, *Cyber Crimes and Law: Cyber Crimes and Law Enforcement* p.73 (Commonwealth, 1st edn., 2002).

[127] Didar Singh, "Electronic Commerce issues of Policy and Strategy for India" (2000)., *available at*: *http*: //www.icrier.orgpdfwp-86.pdf(last visited on March 20, 2013).

1.7. 2. The Information Technology Act, 2000 and Intellectual Property Right Laws

The Information Technology Act, 2000 does not contain provisions relating to Electronic Copyright Management System, Electronic Copyrights, and Protection of Phonogram producers against unauthorized duplication of their Phonograms, etc. The question of copyrights for software programs have not been dealt in the IT Act, 2000. Once the concept of online copyright is included in Indian Intellectual Property Right Legislations performers and makers of phonograms and software producers would be benefited from the following. Namely:

- Legal remedy against misuse of copyright, both direct and indirect in any matter or form, and
- Right of the owner of copyrights to make available to the public programs or performances stores in electronic media, by interactive, on demand, on-line delivery methods.

The internet is the most suitable medium for global trade and exchange of services. The services available in the internet include software, entertainment, information products and professional services. However, many business houses are still wary of conducting extensive business in cyberspace because of the lack of a predictable legal environment governing transactions. Such apprehensions result in concerns about Intellectual Property Protection, Privacy Security and other matters. Commerce on the internet involves the sale licensing of Intellectual Property. To promote an effective environment, sellers must know that their Intellectual Property will not be pirated and buyers must know that they are obtaining authentic products and not pirated copies. For this reason, international agreements that establish clear and effective copyright, patent and trademark protection are necessary to prevent piracy and fraud. While technical means of protection such as an encryption can help prevent piracy, an adequate legal framework is also necessary to penalize piracy and fraud and to provide legal remedies when these crimes are committed. To address these issues, Indian Government should improvise the Intellectual Property Right

Laws (IPR) according to international agreements, in such a way that our national interests are protected and preserved.[128]

1.7. 3. Protection of Copyright in The Legal Regime

The Copyright is the exclusive right to reduce and to perform the work in public or communicate it to the public. Copyright also extends to the exclusive rights to make modifications, adaptations, or translations of copyrighted work. Techniques used on the web include the actions of reproducing and often, modifying and alteration of literary and artistic works (and more recently, musical works). Similarly, the Internet Service Provider (ISP) also use several techniques including caching to provide efficient services.[129] Section 63B which was introduced in the Copyright Act 1957, treats knowing use of infringing copy of computer programs to be an offence. Any person who knowingly makes use on a computer of an infringing copy of a computer program shall be punishable with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees. Provided that where the computer program has not been used for gain or in the course of trade or business, the court may, for adequate and special reasons to be mentioned in the judgment, not impose any sentence of imprisonment and may impose a fine which may extend to fifty thousand rupees.[130]

Section 64 of the Copyright Act, 1957 provides the power to police to seize infringing copies, any police officer, not below the rank of a Deputy Superintendent may, if he is satisfied that an offence under Section 63 of the Copyright Act, 1957 in respect of the infringement of copyright in any work has been, is being, or is likely to be, committed, seize without warrant, all copies of the work, and all plates used for the purpose of making infringing copies of the work, wherever found, and all copies and plates so seized shall, as soon as practicable, be produced before a Magistrate. Any person having an interest in any copies of a work, or plates seized under sub-section (1) may, within fifteen days of such seizure, make an application to the magistrate for such copies (or plates) being restored to him and the magistrate, after

---

[128] V.D. Dudeja, *Cyber Crimes and Law: Crimes in Cyber Space; Scams and Frauds* 72-73 (Commonwealth Publishers, 1st edn.,2002).
[129] *Ibid.*
[130] *Ibid.*

hearing the applicant and the complainant and making such further inquiry as may be necessary, shall make such order on the application, as he may deem fit.[131]

Under section 51 of the Indian Copyright Act, 1957 a person is said to have infringed a copyright when he does anything, which only the copyright holder has the exclusive right to do. Copyright Infringement at attracts criminal liability, the consequences of which are severe and includes fines and imprisonment. The Copyright (Amendment) Act, 1999 covered compliance with Trade Related Intellectual Property Rights (hereinafter referred to as TRIPS). After this massive overhaul, we could boast one of the most modern and forward looking copy right laws in the world, yet like the TRIPs agreement itself these amendments had been enacted in complete of the advent of the internet and of its implication and to that extent have been over taken by events. The new International Content has been created in considerable measure by the world Intellectual Property Organization (hereinafter referred to as WIPO) copyright treaty and WIPO Performance and Phonograms Treaty (PPT) and by the consultation and diplomatic conference held in connection with them and subsequently, though it may not suffice to consider the issues exclusively with reference of these treaties.[132]

The World Trade Organization regime under Trade Related Intellectual Property Rights (TRIPS) puts for the various copyright obligations including:

(i) An obligation to comply with the provision of the Berne conventions.

(ii) A requirement to treat computer programs as literary works for copyright protection purposes and to provide perfection for databases if their selection or arrangement constituting intellectual creations.

(iii) A requirement to give to authors of computer programs and cinematographic works and production of phonograms the right in certain circumstances to control commercial rental of the original or copy of their works.

(iv) An obligation that in respect of works other than phonograms and works of applied art, the normal duration of copy right protection shall be at least fifty year from the death of the author.

---

131 V.D.Dudeja, *Cyber Crimes and Law: Crimes in Cyber Space; Scams and Frauds* p.71 (Commonwealth Publishers, 1st edn.,2002).

132 *Ibid.*

(v) Fair use provisions and similar limitations in the exercise of copyright shall be limited to certain special cases which do not conflict with normal exploitation of a work and do not unreasonably prejudice the legitimate interests of the right holder.[133]

The general question of reproduction in digital form has been taken care of by the 1994 amendment of section 14 (a) of Indian Copyright Act,1957 which confers on the author of a literary dramatic or musical work the exclusive right to reproduce the work in any material form including the storing of it in any medium by electronic means. This extends to computer programs (which are another kind of literary work, vide section 2 (o) of Indian Copyright Act,1957 as provided for in section 14 (b) (i) the definitions of cinematograph film and sound recording contained in section 2 of Indian Copyright Act,1957 are also wide enough to include digital copies of such works. Any of these works on the internet is in digital form, and has been stored in a computer and has therefore been reproduced in material form.[134] The owner of copyright has no monopoly in the subject matters. Others are at liberty to produce the same result (from the common source), provided they do so independently and their work is original. Another person may create another work in the same general form provided he does so from his own resources and makes the work he so originates a work of his own by his own labour and industry bestowed upon it.

Copyright is a right given to or derived from works and it is not a right in novelty only of ideas. It is based on the right of an author, artist or composer to prevent another person from copying his original work. Whether, it is a book, a tune or a picture, which he created himself. There is nothing in the notion of copyright to prevent another person from providing an identical result (and himself enjoying a copyright in that work) provided, it is arrived at or through an independent process.[135]

1.7.3.1. Protection of Computer Software

Software is defined as an act of instructions, which incorporated in a machine readable form is capable of causing a computer to perform a particular task. To put it simply, it is a series of commands, which can be understood by the machine. The

---

[133] *Ibid.*

[134] Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* p.161 (A.P.H. Publishing Corporation, 1st edn.,2003).

[135] *Ibid.*

definition under the World Intellectual Property Organization (WIPO) draft model provision for the protection of computer software comprises of 3 components, viz., computer programme, programme description and supporting material. Going by this definition, it encompasses all aspects of computer software and one could easily cover web pages under this definition. For a computer to function, there are 3 essential types of software, the micro code which is a programme which controls the details of execution, the operating system software which controls the resources of a computer and manages routine tasks and is a necessary requirement for a computer to function and the third is application software which is designed to perform a particular task.[136]

One cannot imagine an internet situation without computers. In fact, it is the computer, which has made the internet possible. In the changed electronic environment, much talked about legal problem is the protection of computer software. A computer software in contrast to a computer hardware, can be defined as an Intangible Property as it is only a set of instructions or commands given to a computer to create a program. It can also be equated with a booklet in the language of the computer, instructing the machine to behave and function according to the instructions given in the booklet. The physical form of these instructions can be embedded in floppy disk, Diskettes, The Compact disc. Random Online Memory (CD-ROM) and is the subject matter of sale in the market. One can say that just like a collection of pages makes a book that is a marketable good but the matter in it is a subject of copyright, similarly the floppy disk, etc. are saleable while the software or the instructions, the programme contained therein cannot be an object of sale. The protection of computer software is necessitated by these factors. Firstly, like any other work of art or creativity, computer software is also the result of one's brain exercise and hence the creator has right over its use by others. Secondly, financial gain of the creator and stopping of its misuse by others has to be controlled, and thirdly, its imitation by others would harm the rights of the creator. There has been an effort worldwide to give protection to computer software in two forms; copyright and patents. In countries like US, software patents are being granted.[137]The key business of the internet is computer software. The largest and most efficient distribution mechanism has existed until date. It is also the largest forum for discussion on

[136] *Id.*at p.172.
[137] Talat Fatima, *Cyber Crimes* pp.34-35 (Eastern Book Company, 1st edn., 2011.).

software and is the largest market and largest producer of software. At the same time, it plays host to the largest number of piracy websites from where one can download software. The issue of computer software piracy is itself not a new one. The term computer software in layman's language means those set of instructions that enable the computer to perform a task. Under Indian Copyright Act, 1957, the term used is computer programme which is defined by section 2 (ffc) as a set of instructions expressed in words, codes, schemes or in any other form, including a machine readable medium, capable of causing a computer to perform a particular task or active a particular result.[138]

The Indian definition is based on the definition of World Intellectual Property Organization (WIPO), draft model provision for legislation in the field of copyright. The definition as under the 1977 Model provision for the Protection of computer software can be said to comprise following three components:

1. Computer programmes,
2. Programme description, and
3. Supporting material

In the 1977, Model law defines the above stated expression as Computer programme means a set of instructions capable when incorporated in a machine-readable medium of causing a machine to take information. Processing capabilities to indicate, perform or active a particular function, task or result. Programme description means a complete procedural presentation in verbal, schematic or other form, in sufficient detail to determine a set of instructions constituting a corresponding computer programme. [139] Supporting material means any material other than a computer programme or a programme description, created for aiding the understanding or application of a computer programme. For e.g. problem description and user instruction.[140]

1.7.3.2. Legal Challenges Pertaining to Software Copyright

With the information super highway, Intellectual Property Protection on the internet has become a major challenge. Before the advent of the internet, software was

---

[138] *Ibid.*
[139] *Ibid.*
[140] Sam Ricketson, "The Berne Convention for the Protection of Literacy and Artistic Works" *Center for Commercial Law Studies* p.896 (1987).

typically stored in a tangible medium like diskettes etc. The internet has replaced these tangible objects and there is no longer the need to have a physical carrier for some types of software. A wide range of information and business are operating through websites. This gives rise to issues of browsing, linking, framing, caching and megatagging etc. which typically would be the infringement of copyright. Before the advent of the internet digital works resided in an identification permanent form such as a disk or hard drive. But now there are virtual documents comprising text, images audio and video clips and these elements may independently qualify for copyright protection. Distribution of software on the internet in a digitized form and not in a physical media and access to software through legitimate means are some of the other challenges posed by the internet on computer software protection.[141]

1.7. 3. 3. Challenges of Software Piracy

Software piracy can be defined as any unauthorized reproduction or acquisition or possession of software. Five distinct types of piracy can be categorized as under:

(1) Enduser Copying (soft lifting)

(2) Reseller piracy

(3) Software rental without permission from copyright holder

(4) internet piracy

(5) Counterfeiting which includes illegally copying, selling illegally copied software and marketing it under a completely different name.

Apart from this categorization, piracy can also be categorized in terms of its scope. In this way, it broadly falls under three categories such as:

(1) Commercial piracy

(2) Corporate piracy and

(3) Home piracy

[141] Tabrez Ahamad, *Cyberlaw E-Commerce and M-Commerce* p.179 (A.P.H. Publishing Corporation, 1st edn.,2003).

The Commercial piracy deals with marketing and distribution of unauthorized software for financial gain. On the other hand, when the officers make additional copies of software without adequate licenses then it is Corporate Piracy. In addition, home piracy as the name suggest is copying software without permission and sharing it between friends and family members etc.

1.7. 3. 3.1. Consequences of Software Piracy

As regards the effects of software piracy, it hinders the development of new software. It also causes loss to the software industry. Software manufacturers are reluctant to enter markets, where piracy rates are high and enforcement action is not effective. It hampers creativity, as there is no incentive to expand time and effort. It also denies the creator of software to give his just reward. Now software manufacturers are paying attention to combat this problem. They are employing physical control and using technology to disable unlicensed versions of software. Software manufacturers have association to increase awareness. They are taking strong actions against the pirates. In India, National Association of Software Companies (NASSCOM) with several steps taken to assist software manufacturers has spearheaded this. The Business Software Alliance (BSA) an association of the top software manufacturers is using International Treaties to combat software piracy.[142]

1.7. E-Commerce and Taxation

The United State and the European Union have reached an agreement on December 5, 1997 to work towards a global understanding that (i) when goods are ordered electronically but delivered physically, there will be no additional import duties in relation to the use of electronic means; and (ii) in all other cases relating electronic commerce, the absence of duties on imports should remain. Subsequently, on February 19, 1998, the US has presented a market access proposal to the World Trade Organization (hereinafter referred to as WTO) General Council calling for agreement among WTO members to maintain current practices not to impose duties on electronic transmissions. The US proposal obviously presupposes that no government considers electronic transmissions to be importations for customs duty purposes and suggests that such duty free status should be maintained in the future also. Moreover, the US proposal treats all electronic transmissions alike irrespective

[142] *Ibid.*

of their content. It is clear that both the initiatives are meant for securing a duty free environment for all electronic transmissions.[143]Instruments of Electronic Commerce include telephone, telex, fax, and even television apart from electronic money transfer. These have been in use for quite some time and have not posed such serious concern in the area of Taxation. However, in recent times, electronic data interchange and particularly the internet have opened up vast possibilities for Electronic Commerce. The internet has not only succeeded in creating a borderless world in the sphere of communication but has also made it possible to transport and deliver a product (both goods and services) so long as the same can be digitalized both within and across the national frontiers. Electronic Commerce over the internet poses various problems before the taxman. Not only the border between what constitutes a good and what constitutes a service becomes thin, it also becomes difficult to determine where the transaction takes place. The buyer may be located in one country, the seller in another and the product may be supplied from a third country. Even the internet address of both the buyer and seller may be located in countries other than the country of their physical location. It may not also be easy to trace all taxable transactions, Moreover, ascertaining the value of the transaction for tax purposes may pose additional problem if the payment details are encrypted.[144]

Taxation issues relating to Electronic Commerce are not confined to levy of customs duties alone. Equally important concerns arise in relation to domestic taxes such as sales tax, value added tax (hereinafter referred to as VAT), and income tax relating to sale of products over the internet. Sales tax or VAT is required to be collected in the country where goods and services are consumed, for convenience; the taxman collects it from the final seller rather than the consumer. In the case of electronic commerce, the product may reach the consumer directly form a seller at a foreign destination. The product may either escape sales tax/VAT altogether or may end up being subjected to double taxation at the hands of the tax authorities of both the countries. Other questions also arise whether the consumer should get sales tax registration. What about the administrative cost involved in tracking individual

---

[143] C Satapathy, "Taxing Electronic Commerce" *Economic and Political Weekly* p.1068 (May 9, 1998).

[144] *Ibid.*

customers. In a federal country like ours, issues relating to inter-state sales tax would also have to be addressed in addition.[145]

Neutrality is a fundamental tenet of taxation. It requires that taxation rules should not affect economic choices and that, therefore, economically similar incomes should be taxed similarly. That is to say that the same taxation principles that apply to income from conventional ways of conducting business should also apply to income from E-Commerce transactions. In cases of cross-border E-Commerce transactions, the tax issues are more complex. According to the recognized principles of International Taxation, when a resident of one country earns income from economic activity in another country, both countries have a right to tax the same income, the home state based on residence rule and the host state based on the source rule of taxation. While the principles of applying the source rule in the case of the conventional method of transactions have been fairly established, those for the E-Commerce transactions pose considerable difficulties.[146]

1.7.1. Taxing Digital Goods in India

Digital goods refers to information-based products that can be digitized and delivered via electronic networks in the form of software, shareware, MP3 music, e-books, photographs, stream video, data, database, etc. Uniqueness of digital goods is in terms of: (a) low cost of production, i.e. duplication or batch production, (b) online delivery of the goods, and (c) faster transaction time. Whether one call downloading an electronic magazine as a service even though the corresponding paper magazine is clearly a good. Under current tax statutes, the paper magazine is taxed while the electronic magazine is not. One could argue that these are essentially the same products, and that their differential treatment under current tax statutes reflects a lack of uniformity that is difficult to defend in a court of law.

Answers to these questions is not easy as countries are still unable to decide whether digital downloads be accorded a status that of a tangible or intangible property, or treated as electronic good or service for the taxation purposes. The differential tax treatment of essentially the same product, in its physical and digital

---

[145] *Ibid.*

[146] Daksha Baxi and Bijal Shah, "Electronic Commerce Taxation Evolves in India" *available at:http://*www.nishithdesai.comfileadminuser_uploadpdfsElectronic_Commerce_Taxation_evolves_in_India.pdf (last visited on February 22, 2012).

manifestations, distorts the uniformity of tax codes. Taxing digital downloads is a difficult proposition as compared to taxing software embedded in a physical medium like a hard drive or the Compact Disc (CD). The concept of subjecting the digital downloads to bit tax has its own limitations as it treats all information downloads equally, whether downloading music or any database. The focus is on how many bits of content has been downloaded. A customer is required to buy from the bit-credits from the Internet Service Provider to be used in downloading the digital contents. Every download is metered by the Internet Service Provider and accordingly bit tax is charged and deposited with the revenue authorities. The problem with bit tax is that it is measured quantitatively rather than qualitatively.[147]

Thus, the question is how to assign tax value to a digital download. One option is to assign a market value (inclusive of tax) to the digital download. Subsequently, the seller deposits the tax component in the account of tax authorities. However, this whole system calls for accounting transparency at the seller's end. In addition, the monitoring or auditing of such electronic activity, however, is difficult because of the fast speed and vast volume of transfer. Moreover, taxation of digital services, would not only involve verification of customer location but also the question as who should be responsible for verification. A trusted third party, like certifying authority may verify the credibility of transaction through digital signatures and certificates.[148]

1.7.3. Taxing Digital (Intangible) Goods

There is no Constitutional provision, central or State tax legislation, which specifically define 'intangible goods'. In the absence of any statutory definition of intangible goods, it would be difficult to extend the expression 'sale or purchase of goods' to cover the 'intangible goods' as well. In *Tata Consultancy Services* v. *State of Andhra Pradesh,*[149] the two Member Bench of S. Rajendra Babu and RC. Lahoti, J), has referred the question whether the branded software, which is an Intangible Intellectual Property, being product of thought, creativity and intellect is classified as 'goods' for the purpose of the Andhra Pradesh General Sales Tax Act, to a Larger Bench. The contention that software is merely 'knowledge' or 'intelligence, and such is not corporeal. Thus, it is not taxable erroneous. Once the 'information' or

147 *Ibid.*
148 *Ibid.*
149 2001 (129) ELT 3 (SC).

'knowledge' is transformed into physical existence and recorded in physical form, it is no longer in intangible form but a corporeal property and hence taxable.

Subsequently, the Constitutional Bench of five judges in *Tata Consultancy Services* v. *State of Andhra Pradesh,*[150] took up the issue whether the canned software which were available off the shelf in the form of software packages sold by the appellants can be termed to be 'goods' and as such assessable to sales tax. The Larger Bench remarked that for the purpose of sales tax, the term 'goods' cannot be given a narrow meaning. In India, the test to determine whether a property is 'goods' for purposes of sales tax, is not whether the property is tangible or intangible or incorporeal. The test is whether the concerned item is capable of abstraction, consumption and use and whether it can be transmitted, transferred, delivered, stored, possessed etc. The Hon'ble Supreme Court's decision has further widened the tax regime to include Intangible Property as well.

E-Commerce represents a paradigm shift and it is hence required that any methodology to tax such a new form of commerce, should be coordinated with the online modalities. The Organization of Economic Co-Operation and Development (hereinafter referred to as OECD) Model Treaty has been one such attempt to recognize such modalities. It is an attempt to provide 'solutions' to the online taxation issues, based on understanding of the digital medium. It would be a fallacy to think that the national domestic laws and the double taxation avoidance agreements in the present form are sufficient in themselves to tackle the problem of online taxation. For example, in the absence of any statutory definition of intangible goods, it would be difficult to extend the expression 'sale or purchase of goods' to cover the 'intangible goods' as well. E-taxation is still in a nascent stage. It needs a systematic approach to understand its various nuances, flexibility in adopting processes and an 'imaginative' collective legislative activity to formulate a set of laws that reflect a common sense approach.

1.8.4. Constituting Permanent Establishment

The tax treatment of cross-border commerce is the subject of bilateral tax treaties, which are often negotiated versions of the Organization of Economic Co-Operation and Development (hereinafter referred to as OECD) Model Tax

[150] AIR 2005 SC 371.

Convention. According to Article 7 of OECD Model, the source country may tax the profits arising from commercial activity carried out within its borders by a foreign entity through a substantial physical presence in the source country. To the justify source of taxation, there must be the level of a 'permanent establishment' by satisfying the following three prerequisites. Namely that there must be a distinct place, such as premises or in certain instances, machinery or equipment ('place-of-business test'), that this must be established with a certain degree of permanence ('permanence test,), and that business must be carried on through the place, usually by personnel of the enterprise ('business-activities test'). If the presence does not reach the level required by the OECD Model by satisfying these requirements, the source state is not entitled to charge income tax on the profits arising from the international transaction. However, the residence country will have the right to tax the profits of its resident.[151]

Moreover, the application and enforcement of traditional tax rules is more difficult in cyberspace than in the brick-and-mortar business world. Events, which would normally give rise to tax liability in the latter world, are likely to escape detection by fiscal authorities in the electronic world and unintentional non-taxation would result. Dotcoms can potentially exploit these new business avenues to gain a competitive tax advantage over their traditional competitors. It is, therefore, evident that governments worldwide must react to this new threat to their fiscal effectiveness.[152]

1.8.4.1. Organization of Economic Co-Operation and Development (OECD) Model Treaty: A Critique

The Organization of Economic Co-Operation and Development (hereinafter referred to as OECD) Model Treaty defines 'permanent establishment' as 'a fixed place of business through which the business of an enterprise is wholly or partly carried on' (Article 5(1)). It defines certain types of activities, per se permanent establishments, including offices, factories, and mines (Article 5(2)). Other types of

---

[151] Parikshit Dasgupta, "India Defining Jurisdictions in E-Commerce Taxations" *available* at: http://www.mondaq.comindiax22619Income+TaxDefining+Jurisdictions +in+Ecommerce+Taxations(last visited on september12, 2012).

[152] *Ibid.*

[152] *Ibid.*

activities are specified as not constituting a permanent establishment for present purposes. The most important of these is the maintenance of a fixed place of business solely for carrying on activity of a preparatory or auxiliary character (Article 5(4) (e)). An enterprise's use of an independent agent to carry on business activities does not create a permanent establishment (Article 5(6)). A permanent establishment does result, however, from use of a dependant agent, one who is acting on behalf of an enterprise and has, an authority to conclude contracts in the name of the enterprise (Article5(5)).

1.8.4.2. Organization of Economic Co-Operation and Development (OECD) Model Treaty and E-Commerce

On December 22, 2000, the Committee on Fiscal Affairs adopted the Commentary on the OECD Model Treaty concerning the issue of the application of the current definition of permanent establishment in the context of E-Commerce (Article5). The Committee has been able to reach a consensus on the various issues concerning the application of the current definition of permanent establishment in the context of E-Commerce. This consensus includes:

- That a website itself cannot constitute a permanent establishment;
- That a website hosting arrangement typically does not result in a permanent establishment for the enterprise that carries on business through that web site; and
- That an Internet Service Provider will not be constituted a 'dependent agent' of another enterprise to constitute a permanent establishment of that enterprise, except in very unusual circumstances.

The Committee concluded that human intervention is not a requirement for the existence of a permanent establishment (PE) because the Committee believes that a requirement of human intervention could mean outside the E-Commerce environment. Important and essential business functions could be performed through fixed automated equipment located permanently at a given location without a Permanent Establishment (PE) being found to exist a result that would be contrary to the object and purpose of Article 5.[153]

[153] Vakul Sharma, *Information Technology Law and Practice* pp.322-323 (Universal Law Publication Co. 1st edn., 2004).

1.8.4.3. Some Changes to the Commentary on Article 5

According to the new OECD Commentary, on the OECD Model Treaty issued on January 28, 2003, a website is a combination of software and electronic data and does not constitute tangible property. Paragraphs 42.1 to 42.10 have been added Commentary on Article 5. It further clarifies:

(a) Whether a website constitutes a place of business,

(b) Whether location of a server constitutes a permanent establishment (PE): when an ISP hosts its website, or when an enterprise owns (or leases) and operates the server on which the website is stored,

(c) Whether the location of computer equipment constitutes a permanent establishment when functions performed through that computer equipment exceeds the preparatory or auxiliary threshold.[154]

1.8.4.4. Whether a Website Acts As a Permanent Establishment

An internet website in itself, which is a combination of software and electronic data, does not constitute tangible property. A website, therefore, does not have a location that can not constitute a 'place of business' as there is no 'facility such as premises or in certain instances, machinery or equipment' as far as the software and data constituting that web site is concerned (Para 42.2 of the OECD Model Treaty)[155].

1.8.4.5. Whether a Server Acts As a Permanent Establishment

The distinction between a website and the server on which the website is stored and used is important since the enterprise that operates the server may be different from the enterprise that carries on business through the website. In order to constitute a fixed place of business, a server will need to be located at a certain place for a sufficient period of time so as to become fixed (Para 42.4 of the OECD Model Treaty).

1.8.4.6 . An Internet Service Provider Hosting A Website

For example, it is common for the website through which an enterprise carries on its business to be hosted on the server of an Internet Service Provider (ISP). Although the fees paid to the internet Service Provider under such arrangement may

---

[154] *Id.* at p.324.
[155] *Ibid.*

be based on the amount of disk space used to store the software and data required by the website. These contracts typically do not result in the server and its location being at the disposal of the enterprise, even if the enterprise has been able to determine that its website should be hosted on a particular server at a particular location. In such a case, the enterprise does not even have a physical presence at that location since the website is not tangible. In these cases, the enterprise cannot be considered to have acquired a place of business by virtue of that hosting arrangement.[156]

1.8.4.7. An Enterprise Hosting Its Own Website

The enterprise carrying on business through a website has the server at its own disposal. For example, it owns (or leases) and operates the server on which the website is stored and used. The place where that server is located could constitute a permanent establishment of the enterprise if the other requirements of the Article are met. Such location may thus constitute a fixed place of business of the enterprise that operates that server. Another issue is whether the business of an enterprise may be said to be wholly or partly carried on at a location where the enterprise has equipment such as a server at its disposal. The question of whether the business of an enterprise is wholly or partly carried on through such equipment needs to be examined on a case-by-case basis, having regard to whether it can be said that, because of such equipment, the enterprise has facilities at its disposal where business functions of the enterprise are performed (Para 42.5 of OCED Model).[157]

Significantly, the commentary further provides, where an enterprise operates computer equipment at particular location, a permanent establishment may exist even though no personnel of that enterprise is required at that location for the operation of the equipment. The presence of personnel is not necessary to consider that an enterprise wholly or partly carries on its business at a location when no personnel are in fact required to carry on business activities at that location (Para 42.6 of OCED Model).[158]

---

[156] Vakul Sharma, *Information Technology Law and Practice* p.325 (Universal Law Publication Co. 1st edn., 2004).
[157] *Ibid.*
[158] *Ibid.*

1.8.4.8. Whether Computer Equipment Exceeding the Preparatory or Auxiliary Threshold Acts As a Permanent Establishment

According to the commentary (Para 42.7 of OCED Model), no permanent establishment may be considered to exist where the Electronic Commerce operations carried on through computer equipment at a given location in a country are restricted to the preparatory or auxiliary activities only. Examples of such preparatory or auxiliary activities include activities, which would generally be regarded as:

- Providing a communications link much like a telephone line between suppliers and customers;
- Advertising of goods or services;
- Relaying information through a mirror server for security and efficiency purposes;
- Gathering market data for the enterprise; and
- Supplying information.

However, such functions form an essential and significant part of the business activity of the enterprise as a whole, or where other core functions of the enterprise are carried on through the computer equipment, and if the equipment constituted a fixed place of business of the enterprise, there would be a permanent establishment (Para 42.8).

1.8.4.9. Internet Service Providers Performing Preparatory or Auxiliary Service

As explained in Para 42.9 of the Commentary that what constitutes core functions for a particular enterprise clearly depends on the nature of the business carried on by that enterprise. For instance, some Internet Service Providers are in the business of operating their own servers for the purpose of hosting web sites or other applications for other enterprises. For these ISPs, the operation of their servers in order to provide services to customers is an essential part of their commercial activity and cannot be considered preparatory or auxiliary.[159]

1.8.4.10. Enterprise Exceeding Preparatory or Auxiliary Threshold

In a case where an e-tailer that carries on the business of selling products through the internet, the enterprise is not in the business of operating servers and the mere fact that it may do so at a given location is not enough to conclude that

[159] *Ibid.*

activities performed at that location are more than preparatory and auxiliary. What needs to be done in such a case is to examine the nature of the activities performed at that location in light of the business carried on by the enterprise. If these activities are merely preparatory or auxiliary to the business of selling products on the internet (for example, the location is used to operate a server that hosts a website which is used exclusively for advertising, displaying a catalogue of products or providing information to potential customers). Then the location will not constitute a permanent establishment. If, however, the typical functions related to a sale are performed automatically at that location, like the conclusion of the contract with the customer, the processing of the payment and the delivery of the products through the equipment located there, then these activities cannot be considered to be merely preparatory or auxiliary.[160] It leads to another condition where The Internet Service Providers (hereinafter referred to as ISP) provide the service hosting the websites of other enterprises on their own servers. The question is whether such ISPs are deemed to constitute permanent establishments of the enterprises that carry on electronic commerce through web sites operated through the servers owned and operated by these ISPs. The Para 42.10 of the Commentary provides that such ISPs are to be treated as independent agents acting in the ordinary course of their business and have no authority to conclude contracts in the name of these enterprises. The United Kingdom, however, has taken the view that in no circumstances servers of themselves or together with websites, constitute permanent establishments of e-tailers.

It is obvious from the above discussion that the Organization of Economic Co-Operation and Development (hereinafter referred to as OECD) Model Treaty has a fixation with fixed place of business or permanent establishments. There exist a number of conditions before a location qualifies for being called a permanent establishment. By referring to a website, as a combination of software and electronic data and does not in itself constitute tangible property, the treaty has negated the concept of virtual office. The changes brought in by the Commentary on Article5 the OECD Model Treaty duly recognize the importance of servers and the performance of core functions being performed at a location (exceeding the preparatory or auxiliary threshold). The concept that a website itself signifies a virtual office by virtue of

[160] *Ibid.*

being visible on the computer screen of a potential customer and constitutes a permanent establishment of the remote seller has its own limitation in the sense that it comes out as an establishment without any fixed co-ordinates. Such a concept is good for business but bad for taxation, as there would always be an incentive to move from high to low (or even zero) tax regime.[161]

1.8.5. Taxation in India: Concept of Business Connection

The term 'taxation' has been defined in Article 366(28) of the Constitution of India in the following terms: 'taxation' includes the imposition of any tax or impose, whether general or local or special, and 'tax' shall be construed accordingly.

The aforesaid Article should be read along with Article 265, which states that: 'no tax shall be levied or collected except by authority of law'. Eligibility to tax is not the same as liability to pay tax. The former depends on the charge created by the Act and the latter on computation in accordance with the provisions in the Act and rules. The Income-tax Act is a standing piece of legislation, which provides the entire machinery for the levy of income tax. Nevertheless, one should not overlook the fact that every year the Income-tax Act is modified or substituted based on the new Finance Act. The Finance Act of each year imposes the obligation for the payment of a determinate sum for each year calculated with reference to that machinery. Thus, the charge to tax would be under the Finance Act in terms of relevant provisions of the Act. It is also a fundamental rule of the law of taxation that unless otherwise expressly provided, income cannot be taxed twice.[162]

1.8.5. 1. When Person is a Resident in India

Taxation in India is based on jurisdictional nexus, source of income and status principles. The principle of jurisdictional nexus determines whether tax can be levied. Source of income is about grouping the income under different heads and taxing them separately and an assessee as defined in Section 2(7) of the Income Tax Act, 1961 means a person by whom any tax or any other sum of money is payable under the said Act.

---

[161] Vakul Sharma, *Information Technology Law and Practice* p.326 (Universal Law Publication Co. 1st edn., 2004).

[162] *Id.* at p.335.

As held by the Supreme Court in *C.1.T.* v. *Shelly Products,*[163] that the Income-tax Act enjoins upon the assessee the duty to file a return of income disclosing his true income. Based on the income so disclosed, the assessee is required to make a self-assessment, to compute the tax payable on such income and to pay the same in the manner provided by the Act. Thus, the filing of return and the payment of tax thereon computed at the prescribed rates amounts to an admission of tax liability which the assessee admits to have incurred in accordance with the provisions of the finance act and the Income Tax Act. As soon as the finance act prescribes the rate or rates for any assessment year, the liability to pay the taxes arises. The assessee is himself required to compute his total income and pay the income tax thereon, which involves a process of self-assessment.[164]

1.8.5. 2. When Company is a Resident in India

Under the Income Tax Act, 1961, a person is a non-resident (S.2 (30)) only if he is not a resident. For individuals, the residential status depends on their physical presence in India and for a company; it depends upon location of the control and management of its affairs. Section 6(3) of the Income Tax Act, 1961, a company is said to be resident in India in any previous year, if

(1) It is all Indian company; or

(2) During that year, the control and management of its affairs is situated wholly in India.

The expression 'Indian Company' has been defined in Section 2(26) the Income Tax Act, 1961, and means a company formed and registered under the Companies Act, 1956. That is, an Indian company is always resident in India even if it is being controlled and managed from outside. In addition, as stated in the previously mentioned sub-clause (ii), a company, which has been controlled and managed wholly from India, is taken to be a resident in India.[165]

The doctrine of the 'control and management' was laid down in *De Beers Consolidated Mines Ltd.* v. *Howe (Surveyor of Taxes).*[166] Generally, the control and

---

[163] (2003) 5 SCC 461.
[164] Vakul Sharma, *Information Technology Law and Practice* p.336 (Universal Law Publication Co. 1st edn., 2004).
[165] *Id.* at p.335.
[166] (1960) AC 455 (HL).

management of a business remains in the hands of a person or group of persons and the question to be asked is where from the person or group of persons controls or directs the business. The real business is carried on where the central management and control resides and not from where the business operations are carried on. Further, in *CTT* v. *Nandlal Gandalal,*[167] the Supreme Court held that control means de facto control and management and not merely the right to control and manage. It is obligatory that for the purpose of taxation. One must also consider the tax treaties signed by India with various countries, which are mainly based on the Organization of Economic Co-operation and Development (OECD) Model. Tax treaties override domestic lax laws with an option to adopt the treaty or the domestic tax law whichever is more beneficial. This results in a relatively lower tax cost for foreign companies whose income is accruing or arising in India. Specifically, income like interest, royalty and fees for technical services are taxed at lower rates than those applicable under the domestic law. Further, these treaties generally provide for complete exemption of profits from operation of ships and aircraft in international traffic.

1.8.5. 3. Establishing Permanent Establishment

In order to tax E-Commerce, it was felt that the expression 'business connection' might not be enough. It led to the constitution of a high-powered committee on Electronic Commerce and taxation by the Central Board of Direct Taxation (CBDT) on December 16, 1999. The objective of the Committee was to examine the growth of E-Commerce business and whether it should be subject to taxation. It had recommended:

(1) That there is no need to define E-Commerce for the purpose of inclusion in the Income Tax Act, 1961.
(2) That the E-Commerce should not be exempted from direct taxation.
(3) That the concept of 'place of effective management' should be continued to be used.
(4) That the concept of the Permanent Establishment (PE) backed by article 5 of the OECD model tax convention should be rejected.

[167] (1960) 40 ITR I (SC).

(5) That the 'Base Erosion' approach in the form of a low 'Withholding Tax' for any payment to a foreign enterprise with the option of being offset by tax on net income by the receiver in his country is a workable option.

(6) That no changes in the Income Tax Act are required until International consensus on abandoning of the Permanent Establishment (PE) concept is reached.

Nevertheless, with the United Nations (UN) and the Organization for Economic Co-operation and Development emphasizing on the merits of PE, it was felt that India should also adopt the concept of Permanent Establishment (PE) in view of rapid globalization of commerce. The Finance Act, 2002 has introduced the definition of Permanent Establishment (PE) in the Income Tax Act. It shall mean to include a fixed place of business through which the business of enterprise is wholly or partly carried on (S.92F (iiia) of the Income Tax Act). It may include a wide variety of arrangements, like a place of management, a branch, an office, a factory, a workshop or a warehouse etc. The definition is similar to that of the United Nations (UN) and OECD models.[168]

1.8.5.4. Establishing Permanent Establishment and the Finance Act, 2003

The Finance Act, 2003 has inserted the section 44DA in the Income Tax Act, to be effective from April 1, 2004. Section 44DA (1) of The Finance Act, 2003 says that the income by way of royalty or fees for technical services received from Government or an Indian concern in pursuance of an agreement made by a non-resident (not being a company) or a foreign company with Government or title Indian concern after the 31st day of March, 2003. Where such non-resident (not being a company) or a foreign company carries on business in India through a permanent establishment situated therein or performs professional services from a fixed place of profession situated therein and the right, property or contract in respect of which the royalties or fees for technical services are paid, is effectively connected with such permanent establishment or fixed place of profession, shall be computed under the head Profits and gains of business or profession. In accordance with the provisions of this Act, provided that no deduction shall be allowed.

[168] Vakul Sharma, *Information Technology Law and Practice* p.336 (Universal Law Publication Co., 1st edn., 2004).

(i) In respect of any expenditure or allowance which is not wholly and exclusively incurred for the business of such permanent establishment or fixed place of profession in India, or

(ii) In respect of amounts, if any, paid (otherwise than towards reimbursement of actual expenses) by the permanent establishment to its head office or to any of its other offices.

(2) Every non-resident (not being a company) or a foreign company shall keep and maintain books of account and other documents in accordance with the provisions contained in section 44AA of Finance Act and get his accounts audited by an accountant as defined in the explanation below sub-section (2) of section 288 and furnish along with the return of income. The report of such audit in the prescribed form duly signed and verified by such accountant.

Explanation – for the purpose of this section,

(a) 'Fees for technical services' shall have the same meaning as in Explanation 2 clause (vii) of sub-section (1) of section 9;

(b) 'Royalty' shall have the same meaning as in Explanation 2 to clause (vi) of sub-section (1) of section 9;

(c) 'Permanent establishment' shall have the same meaning as in clause (iiia) of section 92F.

The Government of India has recently notified (September 2004) that the income tax department will apply the 'arm's length price' principle to determine the profits of a foreign company, earned out of its Permanent Establishment in India providing BPO services. That is, if a foreign company carries on business in India through a Permanent Establishment, its profits will be attributable to the business activities carried out in India and hence will become taxable in India. Further, a foreign company will be treated as having a Permanent Establishment in India if that company carries on business in India through a branch, sales office or through an agent who habitually exercises an authority to conclude contracts, regularly delivers goods or habitually secures orders on behalf of the principal. Thus, it is important to note that the legislatures have started giving due recognition to both Permanent Establishment and business connection for taxing the non-residents. In addition, no attempt has been made to extend either the concept of 'business connection' or the '

Permanent Establishment ' to a website, server hosting a website or Internet Service Provider hosting a website. It seems that the previously mentioned concepts are extendable to include taxing of E-Commerce.[169]

1.8.6. Proposals to Tax E-Commerce and International Cooperation

1.8.6 .1. Bit Tax

One of the most controversial solutions to tax Electronic Commerce was the 'bit tax.' *Arthur J. Cordell* and *Thomas Idea* initially proposed the 'bit tax' in a paper presented at The Club of Rome in December 1994. The tax would apply to all digital 'bits' of information that flow through telecommunications traffic lines that carry interactive digital information. The tax would be applied on the flow volume of bit data and then collected by telecom carriers, satellite networks and cable systems, which would send it directly to governments. The proposal elicited many critical comments. The experts have indicated a number of unanswered questions posed by the 'bit tax' proposal that

- With which transmission there will be subject to tax.
- How intranet transactions will be handled.
- How you are handle redistributions of tax revenues among governments.
- Whether educational, governmental or charitable organizations will be exempt.
- How the inherent pyramiding in wholesale/retail transactions will be eliminated.
- With which jurisdiction will collect the tax, origination or Termination.
- How double tax will be avoided.

The 'bit tax' would very likely burden Electronic Commerce, impeding its growth, eroding its productivity and discriminating against internet users and providers. Nor does it satisfy the tax policy criteria of neutrality and equity. It is not neutral since it is imposed only on digital (as distinguished from non-digital) transfers. It is not equitable since it taxes consumers without regard to the nature of the message being transmitted. A vital medical report would be taxed in the same manner as unsolicited junk e-mail. Bits and bytes are hardly an expression of

[169] *Id.* at p.341.

economic value or wealth. The European Commission rejected the idea of the 'bit tax' and it did not find practical support in the United States.[170]

1.8.6 .2. Trusted Third Parties

The Clinton Administration made a proposal for taxation of Electronic Commerce, which is similar to the traditional Value Added Tax (hereinafter referred to as VAT) scheme. It has been proposed that consumption taxes on E-Commerce could be collected through advanced technologies using third-party collecting agents. Consumers would purchase digital cash cards (also known as smart cards or e-cards) at banks that would allow the seller to identify the country the purchase were made. The VAT would be calculated, based upon the place of consumption and immediately collected with the sale. The seller with a third party escrow agent, who would funnel the money to the appropriate government, would then place the funds. The proposed scheme is a tax-neutral and treats equally both conventional and E-Commerce transactions. In addition to this advantage, the proposal would allow to preserve the consumers' privacy. Because of the importance of the role of escrow agents under the proposal, the crucial factor is credibility of escrow agents. In this respect, the experts identify two main questions: (1) who will be selected to be the escrow agent, and in which country will the agent be located? (2) how will the agent's activities be monitored to ensure the accuracy and the integrity of performance? US trend to adopt residence-based Taxation: Potential Unfairness to Developing Countries as it is extremely difficult to determine the source country in the world of cyberspace. Moreover, E-Commerce complicates the application of the tax threshold concepts of permanent establishment. The U.S. Treasury, in its 1996 report entitled Selected 'Tax Policy Implications of Global Electronic Commerce' proposed a shift from source-based taxation to residence-based taxation.[171]

The growth of electronic commerce opens new possibilities for 'capital flight'. Because the source country possesses the relevant information regarding the earned income, some experts indicate that source-based taxation is more suitable than to prevent the capital flight problem. There is another disadvantage of the residence-based taxation yet, which creates serious doubts about its possible acceptance. The

---

[170] Nuran G. Kerimov, "Current Problems of International Taxation of Electronic Commerce" *available at*: *http://*digitalcommons.law.uga.edu/cgi/viewcontent.cgi ?article= 1023...stu... (last visited on October 12, 2014).

[171] *Ibid.*

residence-based approach in International taxation will put developing countries in disadvantageous position. Due to capital-import nature of developing countries, change from source-based to residence-based taxation could have a major impact on the division of taxing revenues between developed and developing nations. It is not surprising that the United States is among countries that actively promote the idea of a shift to residence-based taxation. In the case of E-Commerce, the United States accounts for an estimated 90% of the world are commercial Web sites (and presumably, therefore, derive a substantial percentage of global revenues from the internet commerce). The United States, therefore, would be the primary beneficiary of a policy endorsing the residence-based taxation of E-Commerce transactions. It is also believed that adoption of residence-based tax system in Electronic Commerce would distort fundamental principles of International taxation (e.g. the primary right of source-country to tax). This approach could be a serious damage to revenues of developing countries and be a major barrier for their development.[172]

1.8.6.3. Tax Administration and International Cooperation

Unique features of electronic commerce complicate enforcement problems for taxing authorities. Unlike transactions with physical goods, E-Commerce of digital goods is hardly be subjected to control and taxation. Taxpayers may disappear in Cyberspace, reliable records and books may be difficult to obtain and taxing points and audit trails may become obscure. It is obvious that traditional mechanisms of control and audit are not fully capable to meet all aspects of E-Commerce. One of the major problems of tax administratively of E-Commerce transactions is determining the taxpayer's identity. If the identities behind E-Commerce transactions cannot be established, they are useless as evidence, even if transaction records and contracts are available to the tax authorities. Tax authorities are already facing and will likely to face the problem of gathering the relevant information related to E-Commerce transactions. E-Commerce is accompanied by corresponding new methods of bookkeeping which are not reliable and can easily be manipulated or even altered. Moreover, tax records are commonly encrypted and tax authorities cannot access them without the decryption key. Experts also indicate another challenge caused by the use of electronic cash. Electronic Cash does not necessitate the use of financial intermediaries by buyers. Unlike traditional business transactions where financial

[172] *Ibid.*

institutions can furnish tax authorities with an audit trail of the transactions, electronic commerce involving the use of electronic cash does not leave audit trails. In cross-border transactions, the tax withholding mechanism is important means of tax collection. Agents (financial intermediaries or legal entities-residents of particular country) usually withhold taxes from payments made to foreign entities. The withholding mechanism may not be of use in electronic commerce transactions where digital products are sold through the internet directly to consumers. There is no need for an intermediary between sellers and buyers. Most of the consumers, especially individuals, have no understanding of their obligation to withhold the relevant taxes from payments made overseas.[173]

The Taxation Framework Conditions agreed in Ottawa in 1998 provides some suggestions to improve tax administration in the sphere of electronic commerce:

- Adopting conventional identification practices for businesses engaged in electronic commerce.
- Developing internationally acceptable guidelines on the levels of identification sufficient to allow digital signatures to be considered acceptable evidence of identity in tax matters.
- Developing internationally compatible information is required, such as acceptance of electronic records, format of records, and access to third party information and other access arrangements and period of retention and tax collection arrangements.

It is important for tax authorities of different countries to co-operate and assist each other in the process of tax collection. The absence of provisions regarding tax collection assistance between countries leaves significant taxes revenues uncollected. The OECD is trying to make changes to the OECD Model Treaty to include tax collection assistance provisions. The OECD has also actively been engaged in developing recommendations regarding tax administration issues of E-Commerce taxation.

[173] Nuran G. Kerimov, "Current Problems of International Taxation ofElectronic Commerce" *available at*: *http://*digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1023...stu... (last visited on October12, 2014).

Conclusion

India comes under the few countries across the world that has enacted E-Commerce legislation. A developing country may become industrialized and modernized if it applies extensively information technology to enhance productivity and International competitiveness, develop E-Commerce and E-Governance applications. A knowledge based society or information-based society is composed of Information Technology products. Many Asian countries in Asia are beneficiary of E-Commerce through opening of economies, which is essential for promoting competition and diffusion of internet technologies. Due to the rapid expansion of internet, E-Commerce plays a very important role in the 21st century, the new opportunities that will be open, will be accessible to both large corporations and small companies. It is the role of government is to provide a legal framework for E-Commerce whereby the domestic and international trade may expand their horizons, basic rights such as Privacy, Intellectual Property, and Prevention of Fraud, Consumer Protection etc. E-Commerce beholds its elements on telephone, computer and web sites which are the basis for deciding competitiveness of a country. India does not perform well on each of them to be a super power in the present century. India must take lead in all relevant areas. It may be assumed that the conduct of business will change very fast, impose further responsibility on India to keep pace with changes by encouraging E-Commerce. We may gain besides lower prices and better quality of information without cost and responsibility of maintaining it.

In the E-Commerce business, the customer will become the real king for which he can decide when to click the mouse, where to click the mouse; and for how much time to click the mouse. Companies have to replace their manual and paper based operations to determine alternatives digital format and simplifying information flow and use their information flows in a dynamic way. E-Commerce may help the companies (smaller or larger) to lower cost drastically across their supply and demand chains, to take their customer service into a different league to enter new markets, to create additional revenue streams and to redefines their business relationships. The internet users in India takes a lot of benefit from internet based E-Commerce, will bring to the fore. Organizations can not only achieve cost reductions but also improve their revenues, and can provide enhanced services by incorporating

E-Commerce. For the individuals can save time by online buying/selling, search costs and can avail best offers/discounts associated with purchase of products/services.

The Indian government tried to fillup gap to cyber law by passing the Information Technology Act, 2000. But some issues are still not covered by the Act which, however, have wide ranging ramification for the growth of E-Commerce in India. The information technology has imposed new legal problems that do not have a precedent in the common law world. The principle of common law has become inapplicable to the legal issue that has evolved in cyberspace, which knows no boundaries and physical environment. These issues do not have any solution in the existing legal regime. However, the Information Technology Act, 2000 tried to fill the gap but in many situation, it becomes not applicable. Thus, the legal positions pertaining to the electronic transactions as well as civil liability for the acts executed in cyberspace is still blur.

The Information Technology Act, 2000, has also not touched payment issue and so there seems no any legal status or validity of an electronic instruction for payment in India. Negotiable Instruments do not include in the applicability of the Act but all transaction concerning with or relating to E-Commerce involving the Negotiable Instruments Act would go to civil courts. The Information Technology Act, 2000 also does not expressly exclude cash and by necessary implication, it may be argued that the Information Technology Act, 2000 would apply in case of cash transaction for E-Commerce. However, actual implication is yet to be seen. In addition, the Information Technology Act, 2000 could not touch the issue of e-transfer of funds. The Information Technology Act, 2000 mentioned about the authentication of the digital signature. Still it is not functional and practical. Hence, govt. should take some effective measures to make the digital signature practical to boost E-Commerce.

Digital Signature can provide a high degree of assurance that a message is originated from a particular person and that its contents could not been altered in transmission. However, no system can provide an absolute guarantee but there seems little doubt that in term of authenticating the terms of a message and the identity of the sender. A well managed system of encryption may be less susceptible to forgery and fraud in comparison to traditional method of contracting.

Intellectual Property Right is complicated areas in the cyber law, but The Information Technology Act, 2000 does not have a word regarding Copyright, Trademarks and Patents. These, however, have wide ranging ramifications for the growth of E-Commerce in India. With the fast developing virtual world, the Intellectual Property Rights have become important as compare to the physical assets. Thus, technological development brings and poses challenges to the basic principles of the Intellectual Property laws. Thus, these challenges are distribution, caching, protection of confidential information, patents, copyrights, trademark and domain names, liability for defamatory statements over networks, content liability and protection, payment mechanism for internet commerce, money laundering, taxation issues, prohibition and regulated activities etc. There has been made amendment in the Intellectual Property laws to fill the gap, which arises due to the technological changes, but it still requires major amendments to deal with the challenges posed by the internet and electronic revolution. Hence India has passed its legislation on E-Commerce namely IT Act, 2000, this enables transactions signed electronically to be enforceable in a court of law.

Many existing doctrines do not have relevancy to cyber space and many issues generated by the advent of the internet could not be adequately answered in the present Copy Right Act. It is to be noted that there is a need to (a) modify the doctrines which constrict the scope of the Copyright Act to traditional media (b) to re-interpret the provision of the Copyright Act which are flexible enough to cover online discrimination of information and (c) amend the Copyright Act so as to plug the loopholes which have been created by the use of cyber space the trademark over the net and its protection is of the heart of the growth of the E-Commerce. The trademark should be registered with the relevant registrar of Trademarks. If the domain name is the trademark, its registration should be done with the concerned registrar for trademarks. Trademark rights of domain name owners are not defined by Information Technology Act, 2000 and the Trademark Act is not fully equipped to deal with web-related trademarks. It is also important to be vigilant in the matter of the violation of trademark. Thus, the internet is a goldmine but without adequate legal protection, it could become a landmine.

CHAPTER II

REGULATORY FRAMEWORK OF E-COMMERCE IN INDIA

Introduction

The internet is a global matrix of interconnected computer networks and the legal framework, which supports commercial transactions, should be consistent and predictable irrespective of the jurisdiction in which a particular buyer and seller reside. Many legal rules assume the existence of paper records and documents, signed records, original records, physical cash, cheques, face-to-face meeting, etc. as long as more activities are carried out by electronic means, it becomes more important as to evidence of these activities be available to demonstrate legal rights and obligations that flow from them. To promote standardization and homogenization of laws internationally, the United Nations Commission on International Trade Law (UNCITRAL) has drafted a Model Law on Electronic Commerce in 1996 to supports the commercial use of international contracts in Electronic Commerce. This Model Law establishes rules and norms that validate Electronic Contracts formed and sets default rules for contract formation and governance of Electronic Contract performance, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence in courts and arbitration proceedings. India was a signatory to the Model Law and is under an obligation to revise its laws inconformity with the said Model Law. There was the urgent need to bring suitable amendments in the existing laws to facilitate Electronic Commerce and to facilitate Electronic Governance, the Information and Technology Act, 2000(hereinafter referred to as IT Act, 2000) was passed. The Act transforms the Model Law into domestic legislation and brings in a procedural infrastructure seeking to regulate this electronic marketplace.

In this chapter, the researcher will look into that The Information Technology Act, 2000 is enacted for legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as Electronic Commerce which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic

filing of documents with the Government agencies and further to amend existing laws. The IT Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. This Act consist of 94 sections divided into 13 chapters and It includes four schedules, which lay down the relative amendments made to the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934. The 13 chapters respectively deal with preliminary matters, digital signature, electronic governance, attribution, acknowledgement and dispatch of electronic records, secure electronic records and secure digital signatures, regulation of certifying authorities, digital signature certificates, obligations of subscribers, penalties and adjudication, the cyber regulations appellate tribunal, offences, network service providers not to be liable in certain cases and miscellaneous provisions. The main aim of this Act is to provide the legal infrastructure for E-Commerce in India. In addition, the cyber laws have a major impact for e-businesses and the new economy in India.

The IT Act, 2000 tries to change outdated laws and deals with cyber crimes. The Act offers legal framework so that information cannot be denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records. The Act provides a legal framework for the authentication and origin of electronic record communication through digital signature. As for as E-Commerce in India is concerned, the IT Act, 2000 contains many positive aspects such as the implications of these provisions for the e-businesses that e-mail would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Digital signatures have become legal validity in the Act. The Act opens the doors for the entry of corporate companies in the businesses of being Certifying Authorities for issuing Digital Signatures Certificates. The IT Act, 2000 provides possible a statutory remedy for corporate in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages.

2.1. The UNICITRAL Model Law On Electronic Commerce And Regulatory Framework Of E-Commerce

The United Nations Commission on International Trade Law (hereinafter referred to as UNCITRAL) was created by the resolution of the General Assembly of

the United Nations in December 1996 in order to streamline, harmonize and unify the law of international trade. Some inadequacies and impediments had crept in the law affecting trade and it became necessary to remove those shortcomings. The draft of Model Law was prepared after debating various proposals in this connection and examining them threadbare, critically and minutely and a copy of the text of the draft Model Law was sent to all governments and international organizations for eliciting their views on the subjects. After examining the comments of the various governments, the Commission adopted the text of the Model Law at its 605th meeting on 12th June 1996. A resolution was passed by the General Assembly on the report of 6th committee and the Model Law on Electronic Commerce came into being to facilitate the use of Electronic Commerce that is acceptable to States with different legal, social and economic system and thus the way was paved for smooth and harmonious international economic relations.[1]

India moved swiftly and promptly in this direction and the Indian Parliament passed the Information Technology Act, 2000 on the pattern of the Model Law on Electronic Commerce (UNCITRAL) adopted by the UN committee on International Trade Law and it came in force on October 17, 2000. This proves the firm determination of the Government of India to make India the IT Super Power by 2008.[2]

The United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Model Law on Electronic Commerce to promote the harmonization and unification of international trade law, so as to remove unnecessary obstacles to international trade caused by inadequacies and divergences in the law affecting trade.[3]The Model Law was prepared in response to a major change in the means by which communications are made between parties using computerized or other modem techniques in doing business (sometimes referred to as trading partners). The Model Law is intended to serve as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of commercial relationships involving the use of computerized or other modern communication

---

1 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.983 (Kamal Law House, Kolkata, 1st edn., 2008).

2 *Ibid.*

3 Sujeet Kumar, *Encyclopaedia of Cyber Laws* p.263 (ABD Publishers, New Delhi, 1st edn., 2011).

techniques, and for the establishment of relevant legislation where none presently exists.[4]

The UNCITRAL Model Law on Electronic Commerce owes its genesis to the report of the Secretary-General entitled 'Legal aspects of automatic data processing', which was examined by the UNCITRAL and which detailed various legal issues relating to the validity of computer records, including issues pertaining to the necessity for 'writing' and authentication of electronic transactions. The UNCITRAL Model Law on Electronic Commerce was drafted in order to serve as a document that the various countries of the world could use to evaluate and amend their own laws and practices and, by providing a common legal platform on which all countries could model their domestic legislations, allows the countries of the world to move towards a uniform international law on Electronic Commerce.[5]

2.1.1. THE UNCITRAL Model Law: A Functional Equivalence Approach

United Nations Commission on International Trade Law (UNCITRAL), which was established by the General Assembly in 1966 to harmonize the law of international trade and intended to facilitate use of Electronic Data Interchange (hereinafter referred to as EDI), e-mail, telecopy, etc. by providing standards by which their legal value can be assessed. UNCITRAL has also produced a Guide to enactment of the Model Law for use by the national governments. The Model Law has a short text of 17 Articles and uses a novel functional equivalence approach. It is based on establishment of functional equivalent of paper-based concepts such as 'writing', 'signature', 'original', etc. The Model Law addresses the question of how to fulfill these functions of paper-based requirements through EDI. It defines 'data message' to mean information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, EDI email, telegram, telex or telecopy.

Article 5 of the Model Law states *that information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.* Article 9 ensures that data messages are admissible as evidence. Articles 6, 7 and 8, respectively, deal with establishing the functional equivalent of paper-based

---

4 *Id.* at p.264.

5 Rahul Malthan, *Law Relating to Computers and Internet* p.182 (Butterworths India, New Delhi,1st edn.,2000).

concepts of *'writing', 'signature'* and '*original'*. Equivalence is conferred subject to standards prescribed.[6]

The lack of legislation in many countries for dealing with E-Commerce as a whole results in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Inadequate legislation at the national level will inevitably create obstacles to international trade. The purpose of Model law was to offer national legislators a set of internationally accepted rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as Electronic Commerce. The Model law seeks to permit States to adapt their domestic legislation to development in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. The Model law thus relies, on a new approach known as the 'functional equivalent' approach which is based on an analysis of the purposes and functions of the traditional paper based requirement with a view of determining how those purposes or functions could be fulfilled through electronic commerce techniques.[7]

The prime aim and object of the IT Act, 2000 is to give effect to the UNCITRAL Model Law, 1996. It is based on the fact that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. The Act has, therefore, been designed to give fillip to functional equivalent approach which provides legal recognition to the electronic counterparts of notion such as *"writing", "signature"* and *"document*. It provides for legal recognition for transactions carried out by means of electronic data interchange and other means for electronic communication (i.e., Electronic Commerce that involve the use of alternatives to paper-based methods of communication and storage of information.[8]

---

6 C Satapathy, "Legal Framework for E-Commerce" *Economy and Political Weekly* p.1906 (July 18,1998).

7 C. M. Abhilash, "E-Commerce Law in Developing Countries: An Indian Perspective" 11(3) *Information and Communications Technology Law* pp.269-270 (2002).

8 B.R. Sharma, Runa Mehta, "Information Technology Act, 2000: An Answer to 21st Century Legal Squabbles" 38(1-4) *Civil and Military Law Journal* pp.135-136 (2002).

The idea behind the Act is to weed out the obstacles arising because of traditional paper-based documentation approach and to create a more congenial and more secure legal environment for Electronic Commerce and encompass computer-based techniques that are able to carry out the similar or same functions. The significant thing to be noted here is that the Act does not attempt to a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria, which, once they are met by data messages enable such data messages to enjoy the same level of recognition as the corresponding paper document performing the same function.[9]The Drafters of the Model law had considered the impracticability of enacting its entire text as a single statute in all countries. Depending upon the situation in each enacting State, the Model law could be implemented in various ways: either as a single statute or in several pieces of legislation. India opted to enact it as one statute called the Information Technology Act, 2000.[10]

2.2. The UNCITRAL Model Law and The Information Technology Act, 2000

The Information Technology Act, 2000 has followed the Model law to a considerable extent. However, there are some areas where it departs from the Model law. The deviations are distinct from the Model law in two key areas: digital signatures and provisions relating to online contracting. These deviations were probably carried out with the legal and economic conditions prevailing in the country in mind.[11]

2.2.1 Electronic Signatures

The definition of electronic signatures in the Model law is well equipped to cope with the rapidly changing technology. Article 7 of the Modal Law states:

> *(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if—*
>
> *(a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and*

---

9 *Ibid.*
10 *Supra not.7* p.270.
11 *Id.* at p.269.

(b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

As this definition does not mention any particular kind of signature (or, in other words, it is technology neutral), it should be understood that as long as an electronic signature meets the test of identification, authenticity and reliability, it is a valid signature. However, the Indian law differs in this respect as the IT Act, 2000 mandates certain technical standards that is, an asymmetric cryptosystem commonly known as '*public key encryption*' and '*hash function*'.

Due to the potential for misrepresentation and fraud that could arise from the use of this method, it was imperative that the generation of key-pairs was entrusted to a Trusted Third Party. The IT Act, 2000 addresses this issue by providing for the licensing of 'Certifying Authorities', who by virtue of the licence obtained from the Controller of Certifying Authorities, may issue Digital Signature Certificates to subscribers. The central government is empowered to prescribe the requirements, which Certifying Authorities are to meet with respect to qualification, expertise, workers, financial resources and other infrastructure facilities. However, the Act itself renders it necessary for Certifying Authorities to have a physical office located in India. In other words, Digital Signature Certificates issued by foreign Certifying Authorities or Trusted Third Parties may not be recognized unless those issuing the certificates have a physical office in India.[12] Although this provision was criticized on the basis that it would discourage foreign Certifying Authorities from offering their services in India, there are, for the time being anyway, at least two advantages of this provision.

2.2.1.1. Legal Perspective

Requiring a physical office in India solves many jurisdictional and procedural problems. Section 47A of the Indian Evidence Act, 1872 as amended in accordance with the IT Act, 2000 deals with the '*relevancy of facts*' with respect to digital signatures. Section 47A of the Indian Evidence Act, 1872 says, "*When the court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the digital certificate is a relevant fact*." In the absence of any

[12] *Id.* at p.272.

international treaty that obliges individual countries to respect each other's certifications, it is a practical approach to have a provision that is feasible and viable.[13]

2.2.1.2. Economic Aspect

In view of the enormous preparations required to set up, Indian Certifying Authorities will take some time to fulfill all the requirements and build up their services. It is vital to protect their interests so that the big fishes do not eat them up. That is not to say that the Government has adopted a closed-door policy to foreign Certifying Authorities. However, it is a reasonable approach to offer everyone a fair and equal opportunity and this provision affords Indian Certifying Authorities a level playing ground with respect to their foreign counterparts. It respects the rights of all the companies concerned.[14]

2.2.2 Electronic Contracts

Any legislation pertaining to E-Commerce will be a futile exercise unless it fills up the lacunae in the existing law regarding the validity of online contracts. Recognizing this factor, the Model law has incorporated a provision in Article 11 relating to the formation and validity of contracts:[15]

> *"In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."*

The IT Act, 2000 as amended now in Section 10-A provides *"where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the grounds that such electronic form or means was used for that purpose."*[16]

---

13 *Ibid*.
14 C. M. Abhilash, "E-Commerce Law in Developing Countries: An Indian Perspective" 11(3) *Information and Communications Technology Law* p.272 (2002).
15 *Id.* at p.273.
16 See, Sec. 10A of The Information Technology Act, 2000.

However, the Indian IT Act, 2000 does not have any express provision regarding the validity or formation of online contracts. In order to understand why, it is pertinent to examine the purpose of Article 11 as well as some basics of Indian Contract Act, 1872. Article 11 is not intended to prescribe a definite standard for the validity of online contracts. It is not the aim of the Model law to interfere with any national law applicable to contract formation. The purpose and scope of Article 11 is outlined in Paragraph 76 of the Guide to Enactment of the Model law:[17] Article 11 is not intended to interfere with the law on formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed. In certain countries, a provision might be regarded as merely stating the obvious, namely that an offer and an acceptance, as any other expression of will, can be communicated by any means, including data messages.

Section 10 of The Indian Contract Act,1872 accords statutory effect to the basic common law principle that

> "*a valid contract may be created if it is made by free consent of parties, competent to contract, for a lawful consideration and with a lawful object and which is not expressly declared void. The Contract Act does not prescribe any particular method for the communication of offer and acceptance"*.

Thus, there is no requirement of writing for the validity of contracts, except in such cases where the requirement of writing is specifically mandated by law. Therefore, the validity of online contracts could not have been challenged solely on technical grounds even before the IT Act, 2000 came into force.[18]

2.3. Objectivity of the Information Technology Act, 2000

The Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) is specially formulated to cover situations arising out of internet transactions and business work online. With the advent of internet communication and techno-logical novices, many legal issues needed attention of the lawmakers and technocrats

---

[17] C. M. Abhilash, "E-Commerce Law in Developing Countries: An Indian Perspective" 11(3) *Information and Communications Technology Law* p.272 (2002).

[18] *Ibid.*

equally and hence, with this object in mind, the IT Act, 2000 is passed to fill the legal vacuum in the field. A perusal of the said statement below would give an original and comprehensive understanding of the IT Act, 2000.[19]

Many legal rules assume the existence of paper records and documents, signed records, original records, physical cash, cheques and face-to-face meetings. Electronic transactions require new forms of record, and recognition of new forms of communication. The Information Technology Act 2000 is pioneering E-Commerce enabling legislations such as the Utah Digital Signatures Act, 1995, the Singapore Electronic Transactions Act, 1998 and the Malaysian Electronic Signatures Act, 1997. The essence of the Act is captured in its long title: 'An act to provide for the legal recognition of transactions carried out by alternatives to paper-based methods of communication and storage of information. The Act comprises three significant aspects[20]:

- Legal recognition of electronic records and communications: contractual framework, evidentiary aspects, digital signatures as the method of authentication, rules for determining time and place of dispatch and receipt of electronic records[21].
- Regulation of Certification Authorities (CAs): appointment of a Controller of CAs, grant of licenses to CAs, duties vis-à-vis subscribers of Digital Signature Certificates, recognition of foreign CAs.
- Cyber contraventions: civil and criminal violations, penalties, establishment of the Adjudicating Authority and the Cyber Appellate Tribunal, and so on. [22]
- The following are the statement of objects and reasons of the IT Act, 2000.[23]

1. New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business.

---

19 Talat Fatima, *Cyber Crimes* p.463 (Eastern Book Company, 1st edn., 2011).

20 Subhajit Basu, Richard Jones "E-Commerce and The Law: A Review of India's Information Technology Act, 2000" 12(1) *Contemporary South Asia* p.13 (March, 2003).

21 Subhajit Basu, Richard Jones "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000" 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at http*://www.bileta.ac.uk/02papers/basu.html (last visited on March 23, 2011).

22 *Supra note*. 20 at p.13.

23 Talat Fatima, *Cyber Crimes* pp.463-465 (Eastern Book Company, 1st edn., 2011).

Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principles hurdles, which stand in the way of facilitating electronic commerce and electronic governance, are the requirements as to writing and signature for legal recognition. At present, many legal provisions assume the existence of paper based records and documents and records, which should bear signatures. The Law of Evidence is traditionally based upon paper based records and oral testimony. Since, Electronic Commerce eliminates the need for paper-based transactions, hence to facilitate E-Commerce, the need for legal changes have become an urgent necessity. International trade through the medium of E-Commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to E-Commerce.

2. The General Assembly of United Nations by its resolution no. A/RES/51/162 on dated 30th January 1997, recommended that all States should consider the said Model Law when they enact or revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Pursuant to a recent declaration by member countries, the World Trade Organization is likely to form a work programme to handle its work in this area including the possible creation of multilateral trade deals through the medium of Electronic Commerce.

3. There is a need for bringing in suitable amendments in the existing laws in our country to facilitate E-Commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures. This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. It is also proposed to provide for a regulatory regime to supervise the Certifying Authorities issuing Digital Signature Certificates. To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislation.

4. With a view to facilitate Electronic Governance; it is proposed to provide for the use and acceptance of electronic records and digital signatures in the Government offices and its agencies. This will make the citizen's interaction with the Governmental offices hassle free.
5. It is also proposed to make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions, which deal with offences relating to documents, and paper based transactions. It is also proposed to amend the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks and the Banker's Books Evidence Act, 1891 to give legal sanctity for books of account maintained in the electronic form by the banks.
6. The proposal was also circulated to the State Governments. They have supported the proposed legislation and have expressed urgency for such legislation.
7. The Bill seeks to achieve the above objectives.

The Act, thus, heralds the paperless world and brings all such activities within the legal fore. It not only legalizes all electronic transmissions but making it legally viable, it also encourages the common man to adapt to the digital situation or the digital mode of information and transaction.

Furthermore, the Act amends the Indian Penal Code, 1860, the Indian Evidence Act, 1872, Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The main purpose of these amendments is to address the related issues of electronic crimes and evidence, and to enable further regulation as regards electronic funds transfers[24]. Unlike similar legislation, the Act also seeks to regulate the internet in some form by making publication of obscene information in electronic form an offence, and for providing offences of hacking and of destroying or altering data. It is also to the credit of the Indian legislature that the Act was one of the first pieces of legislation in India to be thrown open for public comment, prior to it being finalized.[25]

---

[24] Subhajit Basu, Richard Jones "E-Commerce and The Law: A Review of India's Information Technology Act, 2000" 12(1) *Contemporary South Asia* p.13 (March, 2003).

[25] *Ibid.*

2.4. The Silent Feature of I.T. Act

The Act envisages the following salient features:

1. Recognition and protection of paperless transactions.
2. Attribution of electronic messages, i.e. once the message leaves the information system of the originator of messages it is attributed to him.
3. This being a cyber law dealing with commercial transactions, it pointedly gives legal recognition to Digital Signatures, electronic records, electronic filing.
4. Certain online infractions, which can possibly cause a hindrance in the commercial activities, are also enumerated and an elaborate definition of these has been chalked out along with their penalties.
5. Some other offences which are totally new ones and some which come under the category of traditional crimes, but which are now being frequently committed through the medium of the internet are also included along with their penalties. Contraventions regarding electronic records, viz., hacking, theft of electronic records, manipulation of records, spreading viruses, etc. have been defined. Involved in the inquiry and determination of the result of the proceeding is an adjudicating officer, appointed by the Government and possessing wide-ranging powers.
6. As the internet service providers (hereinafter referred to as ISP) are the creators of the internet and as their role in communication of information is crucial, the Act thus secures the position of the ISPs with a view to facilitate free flow of information by absolving them from certain liabilities. Liability of ISPs for content on the internet is limited in so far as the provider exercises all due diligence. This is relevant in connection with copyright violations, pornography, etc., residing on various web pages or moving through the systems of the ISP.[26]
7. Not only that the IT Act, 2000 deals with the substantial part of the issues connected with information technology, it also lays down the procedure and manner of filing complaints, investigation, etc. under the Act and also the powers of authorities concerned and the Tribunals where appeal is to be taken.
8. Privacy, which is the most controversial issue in the internet age, for the first time has a place in the law provisions in India. The breach of confidentiality and

---

[26] Nandan Kamath, *The Law Relating to Computers, Internet and E-Commerce* pp.625-627(Universal Law Publication Co.2nd edn., 2000).

privacy has been made punishable not only with exorbitant fine but even with imprisonment.[27]Privacy and confidentiality of information submitted to statutory authorities and dissemination to third parties of such information collected in pursuance of powers under the Act is made a criminal offence.

9. Secure electronic transactions- these enable parties to enter into Electronic Contracts.
10. Electronic signatures and electronic records given legal status. In furtherance of this, and to maintain security of information, the Act establishes a Digital Signature Infrastructure making specific use of the Asymmetric Crypto System Technology with new authorities such as the Controller of Certifying Authorities being set up.
11. Information Technology Offences, viz., tampering with computer source documents, obscenity - A limited number of offences have been created under the Act. These will be tried as any other criminal offences are under the Criminal Procedure Code but with unique provisions for investigation, search, etc., provided in the Act.
12. Right of government bodies to decrypt information has been specifically given herein.
13. Facilitates E-Commerce as well as electronic filing and maintenance of records as against the government.
14. Setting up of new authorities/regulatory infrastructure - Cyber Regulatory Authorities such as the Controller of Certifying Authorities and the Cyber Regulations Appellate Tribunal (CRAT) have been established. The Act also seeks to set up a Cyber Regulations Advisory Committee (CRAC)

2.5. Concept of Communication Processes: Dispatch and Receipt of Electronic Records

The Indian Contract Act, 1872 lays down that for making a contract, there has to be proposal, assent to the proposal, which transforms into a promise. A promise supported by consideration becomes an agreement and an agreement enforceable by law is contract. It is surprising that over the last hundred years, the law of contract has

[27] Talat Fatima, *op.cit.*pp. 465-466.

remained the same and able to absorb the changes brought in by technology. The IT Act, 2000 has introduced certain statutory conditions pertaining to methodology of contracts formed electronically using computer, computer system or computer network. It highlights crucial aspects of paperless communication leading to formation of contract in real time. In order to appreciate the formation of contract using computer, computer system or computer network, first it would be interesting to understand the communication process involved in effecting a legal contract through post and telephone.[28]

Similarly, the Act has also introduced the concept of Attribution. It provides that an electronic record shall be attributed to the originator if it was sent by the originator himself, or, by a person who had the authority to act on behalf of the originator, or, by an information system programmed by or on behalf of the originator to operate automatically. The Act has established a presumption that under certain circumstances a data message would be considered as message of the originator. It allows the use of functional acknowledgements, which would parallel the system known as Registered Post Acknowledgement Due (RPAD) in the conventional postal systems. The Act addresses the legal issues arising from the use of acknowledgement procedures. Time and place of dispatch and receipt of electronic record have been ascertained. The Act envisages some basic principles for the determination of the time of receipt. Both determination of time of dispatch and time of receipt have been made dependent on the definition of entry into the information system.[29]

2.5.1. Understanding Communication Processes

For a contract to happen there should be a communication of proposal and communication of acceptance as well. The postal rule lays emphasis on both communication of proposal and communication of acceptance. A contract comes into existence when the acceptor puts his acceptance/ accent into transmission so as to be out of the power of the said acceptor. Contract through post/ correspondence is complete at the place where acceptance is made. The acceptance gives rise to the cause of action and not merely the making of all offers. Consequently, a posted

---

[28] Vakul Sharma, *Information Technology : Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.48 (Universal Law Publishing Co. Pvt. Ltd., 2nd edn., 2007).

[29] B.R. Sharma, Runa Mehta, "Information Technology Act, 2000: An Answer to 21st Century Legal Squabbles" 38 (1-4) *Civil and Military Law Journal* p.136 (2002).

acceptance will be effective on posting, although that will not be the case if it goes astray because the offeror has not addressed it properly, or if the acceptor has specified that any acceptance will not be effective unless he or she, has received it. The contract is concluded when the letter of acceptance is posted. If the letter of acceptance reaches later than usual then that does not entitle the offeror to allege that he is not bound by the contract. It has been argued that the 'postal rule' is harsh on proposer/offeror and no matter whether it was the delay or negligence on the part of the postal department, it is the proposer/offeror who suffers.[30]

The applicability of 'postal rule' was put to test in *Entores Ltd.* v. *Miles Far Eastern Corporation*[31] wherein the plaintiff, in London, made an offer by telex to the agents of the defendant corporation, in Holland. This was accepted by a telex, which was received on the plaintiff's telex machine in London. The relevant issue was whether the contract was made in England. If it were, that would provide a basis for the plaintiffs to serve a writ on the defendant corporation outside of the jurisdiction. The court held that the contract was made in London. *Denning, L.J.*, who delivered the principal judgment of the Court observed:

> "*When a contract is made by post it is clear law throughout the common law countries that the acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. But there is no clear rule about contracts made by telephone or by telex. Communication by these means is virtually instantaneous and stands on a different footing*".
>
> He concluded: "*That the rule about instantaneous communications between the parties is different from the rule about the post. The contract is only complete when the acceptance is received by the offeror and the contract is made at the place where the acceptance is received*".

A similar view was expressed by the Supreme Court in *Bhagwandas Gouerdhandas Kedia* v. *Girdharilal Parshottamdas and Co*[32] In this case, the plaintiffs commenced an action in the City Civil Court at Ahmedabad against the Kedia Ginning Factory and Oil Mills of Khamgaon (defendants) for a decree of Rs. 31,150/- on a plea that the defendant had failed to supply cotton seed cake, which they had agreed to supply under an oral contract dated July 22, 1959 negotiated between

---

30 Vakul Sharma, *op.cit.* p.48.
31 (1955)2 QB 326.
32 AIR 1966 SC 543.

the parties by conversation on long distance telephone. The plaintiffs submitted that the cause of action for the suit arose at Ahmadabad, because the defendants had offered to sell cotton seed cake, which offer was accepted by the plaintiffs at Ahmadabad. The decision by majority view was that telephone is an instantaneous mode of communication, just as if the parties were in presence of each other.

The exception to the general rule, as applied to post, would not apply here. So, in this case, the contract would be made at the place where acceptance is received, i.e., Ahmadabad. It is clear from the aforesaid judgments that the courts have reinterpreted the contractual obligations of offeror/acceptor by evaluating the technological applications. It is established law that the contract is complete only when the acceptance is received by the offeror and the contract is made at the place where the acceptance is received (instantaneous communication rule).[33]

Postal rule	**Instantaneous communication rule**
Contract through post/ is correspondence Complete when the acceptor puts his acceptance /assent into transmission to be out of the power of the said acceptor and the contract is made at the place where acceptance is made.	Contract through telephone/telex/fax is Complete when the acceptance is received by the offeror and the contract is made at the place where the acceptance is received.

Table 5.1: Postal Rule v. Instantaneous Communication Rule[34]

Mere mechanical application of either 'postal rule' or 'instantaneous communication rule' without taking into accounts the facts and circumstances would be fallacious. It is held by the Supreme Court in *Bank of India* v. *O.P. Sioarnakar*[35], that the law relating to "offer" and "acceptance" is not simple. The said judgment quoted, Geneally G. Gilmore- (1974):

---

33 Vakul Sharma, *op.cit.*pp.50.
34 *Ibid.*
35 (2003) 2 SCC 721.

"The rules of offer and acceptance are usually favorites of law students. They are easily stated and tend to be rather mechanical in their operation. They also involve situations that are relatively easy to grasp and in which various policy consideration are close to the surface. However, one should not assume that one has mastered the law of contracts simply because one is conversant with rules of offer and acceptance. Indeed the writings of modem contracts scholars tend to deprecate the importance of the rules of offer and acceptance".

The IT Act, 2000 has not amended or substituted the Indian Contract Act, 1872 in any manner whatsoever. In order to form a valid Electronic Contract one still needs a '*promisor*' and a '*promisee*". The Act grants legal recognition to communication process involving computer, computer system and computer network by identifying attribution, acknowledgement and dispatch of electronic records as key statutory provisions.[36]

2.5.2. Parties to the Communication Process

The Act identifies three parties to the electronic transmission process: the originator,[37] the intermediary[38] and the addressee.[39] All three parties perform specific functions with respect to an electronic message. Originator sends, generates, stores or transmits any electronic message; whereas, intermediary is a facilitator who on behalf of another person receives, stores or transmits or provides any service with respect to that message; and addressee is the recipient of that message (record).[40]

The Act recognizes that three parties may exist in connection with a data message.

- Tile Originator is the person who sends, generates, stores or transmits the electronic message or causes it to be sent, generated, stored or transmitted to any other person.[41]
- Tile Addressee is the person who is intended by the originator to receive the electronic message.[42]

---

36 Vakul Sharma, *op.cit.*pp.50.
37 See, Sec. 2(1)(za) of the Information Technology Act, 2000.
38 See, Sec. 2 (l)(w) of the Information Technology Act, 2000.
39 See, Sec. 2(1)(b) of the Information Technology Act, 2000.
40 *Id.* at p.51.
41 See, Sec. 2(1)(za) of the Information Technology Act, 2000.
42 See, Sec. 2(1)(b) of the Information Technology Act, 2000.

- The Intermediary, with respect to a particular electronic message is any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message.[43]

One will note that the definition of originator covers not only the situation where information is generated and communicated, but also the situation where such information is generated and stored without being communicated. However, the definition of originator is intended to eliminate the possibility that a recipient who merely stores a data message might be regarded as an originator.[44] In addition, the definition of addressee contrasts with the definition of originator, which is not focused on intent. It should be noted that, under the definitions of originator and addressee, the originator and the addressee of a given data message could be the same person, for example in the case where the data message was intended for storage by its author.[45]

The definition of intermediary is intended to cover both professional and non-professional intermediaries, i.e., any person (other than the originator and the addressee) who performs any of the functions of an intermediary. It will be noted that intermediary under the Act is defined not as a generic category but with respect to each data message, thus recognizing that the same person could be the originator or addressee of one data message and an intermediary with respect to another data message.[46]

2.5.3. The Concept of Attribution

Section 11 of IT Act, 2000 deals with the attribution of electronic records. It lays down three conditions as to when an electronic record shall be ascribed to a person who sends generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person. Such a person is known as an originator. The Section 11 of IT Act, 2000 laid down conditions in this regard are as under-

(a) Such electronic record must have been sent by the originator himself, or

---

43 See, Sec. 2(1)(w) of the Information Technology Act, 2000.

44 Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.630 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

45 *Ibid.*

46 *Id.* at p.631.

(b) It must have been sent by a person who had the authority to represent or act on behalf of the originator in respect of that electronic records; or

(c) It must have been sent with the help of an information system, which was programmed by or on behalf of the originator to operate automatically.

According to Section 2(1)(za) of IT Act, 2000, *a person, who has authority to act on behalf of the originator, does not include an intermediary.* As regards clause (b) of this Section, Section 88A of the Indian Evidence Act, 1872, in its last leg, says that the court shall not make any presumption as to the person by whom such message was sent.[47]

In the case, *L.M.S. Umma Salemma* v. *B.B. Gujaral*[48] the Supreme Court held that the court may refuse to make any presumption. The Apex Court held that the court may, initially draw a presumption but after considering the evidence adduced before it, it may derive such a conclusion which is against the presumption.

2.5.4. Acknowledgement of Receipt of Data Message

In Electronic Contracts, technology permits the use of functional acknowledgments, which would parallel the system known as Registered Post Acknowledgment Due (RPAD) in the conventional postal systems. The Act does not impose the use of any such procedure. However, taking into account the commercial value of a system of acknowledgement of receipt and the widespread use of such systems in the context of Electronic Commerce, the Act addresses the legal issues arising from the use of acknowledgement procedures.The provision of the Act dealing with acknowledgment of receipt is based on the assumption that acknowledgement procedures to be used at the discretion of the originator. In cases where the originator has not agreed with the addressee that the acknowledgement of receipt is to be given in a particular form, the acknowledgement may be given by any communication by the addressee or conduct by the addressee which is sufficient to indicate to the originator that the electronic record has been received.[49]

---

47 R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1011 (Kamal Law House, Kolkata, 1st edn., 2008).

48 (1981)3 SCC 317.

49 Nandan Kamath, *op.cit.* p.632.

In Section 12 of this Act, the acknowledgement of receipt of an electronic record has been dealt with. According to it, there are various modes by which receipt of an electronic record may be acknowledged.

> Section 12(1) says that: *where in a case, the originator has not agreed with the addressee that the acknowledgement of receipts of an electronic record be given in a particular form or by a particular method, an acknowledgement may be given by the following two ways-*
>
> *(a) Any communication by the addressee automated or otherwise; or*
>
> *(b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.*[50]

2.6. Time and Place of Dispatch and Receipt of Electronic Records/ Messages

The Act defines the time of dispatch (dispatch refers to the commencement of the electronic transmission of the data message) of an electronic record/message as the time when the data message enters an information system (either designated or not) outside the control of the originator, which may either be the information system of an intermediary or an information system of the addressee[51].

For determining the time of receipt, the Act lays down some principles.

- *If the addressee does not designate any computer resource for receipt of the record/message, receipt of the record/message occurs when the electronic record enters the computer resource of the addressee*
- *If the addressee has unilaterally designated a computer resource (in which case the designated system may or may not be an information system of the addressee) for the purpose of receiving electronic records/messages receipt occurs at the time when the electronic record/message enters that designated computer resource.*
- *The Act also addresses the situation where the addressee designates a specific information system for the receipt of the record/message, and the data message reaches an information system of the addressee that is not the designated system. In such a situation, receipt is deemed to occur when the addressee retrieves the data message. It is important to note that, for the purposes of this section, the mere indication of an electronic mail or telecopy*

---

50 R.K. Chaubey, *op.cit.*p.1012.

51 See, Sec. 13 of The Information Technology Act, 2000.

address on a letterhead or other document should not be regarded as express designation of one or more information systems.[52]

This is a replica of Article 15 of the Model law. Some commentators hold that Section 13 modifies the existing substantive provisions of the Indian Contract Act. Section 13 only explains and clarifies, inter alia, when the dispatch and receipt of electronic records take place and is meant purely for ascertaining the time of dispatch and receipt of information, which is a relevant factor in many contracts. This Section, in fact, reflects the 'functional equivalent' approach adopted by the Model law, which does not seek to alter national law applicable to contract formation, but only aims to provide electronic communications with the same degree of legal certainty as paper-based communications.[53]

Section 13 of the IT Act, 2000 therefore, only offers a framework for understanding the formation of E-Contracts in India. It does not, in any way, alter or modify the existing substantive law of contract. In order to ascertain the formation of Electronic Contracts, one has to read Section 13 together with Section 4 of the Contract Act, which enunciates certain rules regarding the communication of proposals, acceptance and revocation:[54] The communication of a proposal is complete when it comes to the knowledge of the person to whom it is made. The communication of an acceptance is complete, as against the proposer, when it is put in a course of transmission to him, so as to be out of the power of the acceptor; as against the acceptor, when it comes to the knowledge of the proposer … Section 13 of the IT Act, 2000 comes in handy when applying these rules to E-Contracts.[55]

For example, in the case of an acceptance made by an electronic record, a combined reading of the two sections will evolve the following rules. The communication of an acceptance is complete as against the offeror, when the electronic record is dispatched such that it enters a computer resource outside the control of the originator (acceptor) and as against the acceptor, when the electronic record enters any information system designated by the offeror for the purpose, or, if no system is designated for the purpose, when the electronic record enters the

---

52 Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.634 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

53 C. M. Abhilash, "E-Commerce Law in Developing Countries: An Indian Perspective" 11(3) *Information and Communications Technology Law* pp.269-281(2002).

54 *Ibid.*

55 *Ibid.*

information system of the offeror, or, if any information system has been designated, but the electronic record is sent to some other information system, when the offeror retrieves such electronic record. Similarly, Section 13 can be applied to any of the rules of Section 4 of the Indian Contract Act and it evolves that it does not alter any existing principles of Contract Act.[56]

However, the Supreme Court of India, recognizing the distinction between 'postal rules' and 'receipt rules' as elaborated in *Bhagwandas* v. *Girdharilal*,[57] following the English decision in *Entores Ltd* v. *Miles Far East Corporation*[58], had held that Section 4 is applicable only in non-instantaneous forms of communication and does not apply to instantaneous forms of communication. Therefore, it may be noted that this method is useful only for non-instantaneous forms of communication as contracts concluded by E-mail and may be inapplicable in instantaneous forms like 'web click' contracts. In the case of instantaneous forms of communication, it has been held that a contract is formed when the offeror receives the acceptance. Therefore, in the virtual world, an offer or acceptance is complete when the addressee is in receipt of the electronic record as defined in Section 13(2) of the IT Act, 2000.

2.6.1. The Meaning and Concept of Dispatch of An Electronic Record

A sends B an e-mail with attached MS-Word files. A had used a 'WinZip' software to compress the files for faster transmission over the internet. B received the 'WinZip' file sent by A but he failed to read it as his computer did not have the necessary 'WinZip' software to 'unzip' the compressed files. Hence, it is important that for successful communication process of the electronic records, there shall be an agreement between the originator and the addressee about the use of specific software in creation and dispatch of the electronic records.[59]

The section 13(2) states a situation where the addressee has already designated a computer resource for the purpose of receiving electronic records. The receipt occurs at the time when the electronic record enters the designated computer resource or it may so happen that the originator sends the electronic record to a non-designated computer resource then in such a case receipt occurs at the time when the electronic

---

56 *Ibid.*
57 1966 AIR SC 543.
58 (1955) 2 QB 327.
59 *Id.* at p.55.

record is retrieved by the addressee. It presumes that the originator has a prior knowledge of the addressee's designated computer system.[60]

2.6.2. Identifying The Designated Computer Resource

An addressee (or originator) needs a computer resource to receive (or send) the electronic record. For example, *abc@satyam.net.in* represents an email id of a person having identity *abc, and satyam.netin* as his computer resource (network). If the person (addressee) informs the other party (originator) that his email id is *abc@satyam.net.in,* then the said email id will become his designated computer resource. Emails ids given on the visiting cards/business cards, letterheads, websites etc. should be taken as examples of designated computer resources. The clause (b) of the aforesaid sub-section13 (2) states a situation where the addressee has neither designated a computer resource nor any timings for the purpose of receiving electronic records. The receipt occurs when the electronic record enters the computer resource of the addressee.[61]

2.6.3. Place of Business

According to sub-section (3) of Section 13, if there is no otherwise agreement between the parties, herein we have the originator and the addressee, an electronic record is deemed to have been sent off at his place of business, and it is deemed to have been received at the place where the sender (addressee) has his place of business. Place of business ordinarily means a location where one carries on one's business. Herein for the purposes of this sub-section, place of business is meant by a place from where the originator can send an electronic record just as MP3 audio file, SMS, MMS, E-mails etc. by the means of a mobile phone and the like devices.[62]

Sub-section (4) of Section 13 lays down that the provisions of sub-section (2) shall apply despite the fact that the place, where the computer resource is located, may be different from the place, where the electronic record is deemed to have been received under sub-section (3) of this Section 13. Actually, what the provisions of sub-section (4) intends to convey is that the location of computer resource has no relevancy as such. These provisions shall have no effect on the provisions of sub-

---

60 *Id.* at p.56.
61 *Ibid.*
62 R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1015 (Kamal Law House, Kolkata, 1st edn., 2008).

section (2), wherein the time of receipt of an electronic record is determined by adopting different ways; and on the provisions of sub-section), wherein it has been discussed as to when an electronic record is deemed to be dispatched at the place where the originator has his place of business and, it is deemed to be received at the place where the addressee has his place of business.[63]Sub-section (5) of section 13 deals with explanatory meaning of place of business as discussed in the provisions of sub-section (3) thereof. Therefore, it should be read and understood in the context of the provisions of sub-section (3). Sub-section (5) has been divided into three separate clauses with a view to explain the meaning of the terms place of business. Clause (a) says that where the originator or the addressee carries on his business at more than one place, than place of business shall be the place where the head office" of his business is located. Clause (b) provides that in a case where the originator or addressee has no place of business in that circumstance, his place of business shall be deemed at a place where he usually resides. i.e. where his usual place of residence is located. Clause (c) takes usual place of residence in context to body corporate, which means the place where it has been registered for the purpose of post of correspondence, or official communications, etc.[64]

2.7. Legal Regulation of Several Certifying Authorities

Internet is an open system of communication, which has its own set of problems. These problems relate to integrity, confidentiality and authentication of communication channels and processes. Since, the computerized environment is more process based than personalized, it is hence necessary to have an identification strategy to ascertain the integrity, confidentiality and authentication of communication channels and processes. Trusted third parties, which will not only authenticate that a digital signature belongs to a specific signer but also, dispense the public keys. That trusted third party is referred to as a certification authority. Its function is to verify and authenticate the identity of a subscriber (a person in whose name the Digital Signature Certificate is issued). A certifying authority has to receive a licence from the root certifying authority or controller of certifying authorities, before it starts issuing digital signature certificates to the subscribers. The issuing certification authority's digital signature on the digital signature certificate can also be verified by using the

---

63 *Ibid.*

64 *Id.* at p.1016.

public key of the certification authority listed in the repository of root or controller of certifying authorities.[65]

The IT Act, 2000, in order to give impetus to the electronic activities and to secure electronic signatures, devises the ways and means to achieve reliability in this regard. Thus, it envisages its own legal infrastructure to ensure trustworthy relations online. This is done by establishing the Public Key Infrastructure (PKI) in which hierarchy of authorities is its main feature. The authorities at the apex, namely, the Controllers empower the Certifying Authorities by issuing licence to them to issue Electronic Signature Certificate. The Controllers enjoy superintendence over the Certifying Authorities.[66]

The Supreme Court in *A. K. Kraipak* v. *Union of India*[67] observed:

> "*The dividing line between an administrative power and a quasi judicial power is quite thin and being gradually obliterated. For determining whether a power is an administrative power or a quasi judicial power one has to look to the nature of the power conferred, the person or persons on whom it is conferred, the framework of the law conferring that power and the manner in which that power is expected to be exercised. Under our Constitution, the rule of law pervades over the entire field of administration. The requirement of acting judicially in essence is nothing but requirement to act justly and fairly and not arbitrarily or capriciously*".

2.7.1. Controlling Authorities and Their Appointment

Section 17 of The Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) empowers the Central Government to appoint a Controller of Certifying Authorities and appoint such number of Deputy Controllers, Assistant Controllers, other officers and employees as it deems fit. Such appointment is to be notified in the Official Gazette. According to Section 17 of the IT Act, 2000, the Deputy Controllers, Assistant Controllers and other officers and employees shall be under the general supervision of the Controller while the Controller shall be subject to the general control and directions of the Central Government. The Central Government shall such as prescribe the qualifications, experience, terms, and

---

65 Vakul Sharma, *op.cit.* pp.61-62 .
66 Talat Fatima, *Cyber Crimes* p.469 (Eastern Book Company, 1st edn., 2011).
67 (1969) 2 SCC 262.

condition of service of Controller, Deputy Controllers, Assistant Controllers, other officers and employees. The head office and the branch offices of the Controller shall be established on the direction of the Central Government. The office of the Controller shall also bear a seal.[68]

> In the case of *A.K. Kraipak* v. *Union of India*[69] it was observed by the Supreme Court that, every organ of the state under our constitution is regulated and controlled by the rule of law.... *"The concept of rule of law would lose its validity if the instrumentalities of the State were not charged with the duty of discharging their functions in a fair and just manner. The requirement of acting judicially in essence is nothing but a requirement to act justly and fairly and not arbitrarily or capriciously."* Thus, we should view this Section in the above context.

2.7.2. Functions of Controller

Section 18 of this Act deals with the functions of the Controller in connection with the certifying Authorities, which may be prescribed by regulations. The clause (a) of this section provides that the Controller may supervise the activities of the Certifying Authorities. According to clause (b), he may certify public keys of the Certifying Authorities clause (c) says that the Controller may lay down the standards for the Certifying Authorities. He may specify the qualifications and experience for the staff of Certifying Authorities (clause (d), Clause (e) of this Section 18, says that the controller has got right to specify the conditions for the conduct of the business by the certifying Authorities. Clause (f) provides that the Controller may also specify the contents of written, printed or visual materials and advertisements, which are used in connection with a Digital Signature Certificate and public key.[70]

Besides, the Controller has got a right to discharge several other functions (clauses (g) to (n)) like, he may specify the form and contents of a Digital Signature Certificate and the key, he may specify as to what will be the form and manner for maintenance of the Accounts by the certifying Authorities, he may also specify the terms and conditions for the appointment of the Auditors and for the remuneration which are to be paid to them. The controller facilitates the establishment of any

---

68 Talat Fatima, *op.cit*.p.469.
69 (1969) 2 SCC 262.
70 Talat Fatima, *Cyber Crimes* p.471 (Eastern Book Company, 1st edn., 2011).

electronic system, a certifying authority. He may specify the manner of dealings with the subscribers to be conducted by the certifying Authorities. The controller has to solve the dispute, if any, arising between the certifying Authorities. He may also tell the certifying Authorities about their duties. He maintains a database, which shall contain the disclosure of the record of every certifying Authority containing such particulars as, may be specified by regulations.[71] Thus, the Controller has a large area of functions which are almost all related to the Certifying Authorities. It is to be noted here that in the unamended IT Act, 2000, the Controller was to be the repository of all Digital Signature Certificates under Section 20, which has now been omitted by the IT (Amendment) Act, 2008.[72]

2.7.3. Certifying Authority

Certifying Authorities can be termed as the backbone of the Public Key Infrastructure (hereinafter referred to as PKI). They are like a hyphen, which joins, a buckle, which fastens the subscriber to the Controlling Authority. They originated as Trusted Third Parties (TTPs) and are primarily instrumental in cryptographic key management, identification of a party to a transaction. They lend authenticity to the electronic signature, thereby making the electronic message, public keys reliable. Electronic certificates are messages that are signed with the Certification Authority's private key. It is a trusted member of the PKI family and has power not only to issue the Electronic Signature Certificate but also to revoke the same.

Besides the importance of the Certifying Authorities in the PKI, it is also important to make the position of the Certifying Authority a promising one. To achieve this, Certifying Authority must have the following attributes:

1. It must have independence and should work without unnecessary restrictions;
2. Internal security is necessary for the Certifying Authority;
3. Viability and stability must be maintained as evidentiary needs may arise after a long gap of time;
4. There should be existence of a contingent plan;
5. Expertise and knowledge in the technology of encryption and decryption;
6. Securing its own private key;

---

[71] *Id.* at pp.1022 -1023.
[72] Talat Fatima, *op.cit.*p.471.

7. Must be equipped with revocation procedures;
8. Insurance;
9. Interaction with foreign certification authorities; and
10. Personal selection and reliable management.

Thus, it is evident that the IT Act, 2000 has well equipped the Certifying Authority. As in the world of cyberspace, nothing can be local hence, only cross-border preparation can bring success in any of the internet-related provisions. For this reason, to accomplish international dealings lawfully Section 19 of the IT Act, 2000 gives recognition to the foreign Certifying Authorities. This power has been given to the Controller with certain prescribed restrictions that after the approval of the Central Government, the Certifying Authority shall recognize any foreign Certifying Authority as a Certifying Authority for purposes of the Act. However, like any other Certifying Authority under the IT Act, 2000, the foreign Certifying Authority's recognition is placed at the will of the Controller. Thus, if the Controller is satisfied that the conditions and restrictions on the basis of which the foreign Certifying Authority was given recognition has been violated by it, then he may after recording the reasons revoke its recognition and notify the same in the Official Gazette (Section 19(3)).[73]

2.8. Legal Recognition of Foreign Certifying Authorities

Section 19(1) of the IT Act, 2000 makes provisions for the power to the Controller to grant recognition to foreign certifying Authorities by obtaining approval of the Central Government and subject to such conditions and restrictions as may be specified in the regulation. Sub-section (1) further provides that the controller has got a right that it may, by a notification in the official Gazette, recognize any foreign certifying Authority as a certifying Authority for the purpose of this Act which are very wide such as for a faster implementation of digital signature certificates scheme, and legislative intention of the parliament to enact this Act.[74]

The legislative intention, in this regard, is two-fold-firstly, the enactment of such a nature should not ignore the national or municipal perspectives of information technology, and secondly, the enactment should have an international perspective as supported by the UNCITRAL Model law. Thus, the Act is not only in conformity

[73] *Id.* at pp.469-471.
[74] *Id.* at pp.469-471.

with the said model law on E-Commence, but it also reveals aspects or information technology for the promotion of efficient and quicker delivery of Government services by means of reliable electronic records. Sub-section (2) of Section 19 provides that where any Certifying Authority is recognized under sub-section (1), the Digital Signature Certificate issued by such certifying Authority shall be valid for the purposes of this Act. Herein, a recognized Certifying Authority means such a person who is granted a licence to issue a Digital Signature Certificate under the provisions of Section 24 of this Act. According to the provisions of sub-section (3) of section 19, if the controller feels satisfied that a Certifying Authority has violated any of those conditions and restrictions under which it was conferred recognition as per sub-section (1) of this section, he has got a power to cancel such recognition. Moreover, for this cancellation, he will assign the reasons in writing and he needs to notify it by a notification in the official Gazette.[75]

The aforesaid sub-section (2) refers recognition of any foreign Certifying Authority as a Certifying Authority by the Controller. The term recognition implies that the Controller shall grant licence to any foreign certifying authority to act as a licensed CA in India subject to such conditions and restrictions as may be specified by Information Technology (Certifying Authorities) Regulations, 2001. The Controller has the power under aforesaid sub-section (3) to revoke the recognition granted to the foreign Certifying Authority under sub-section (2), if fl he is satisfied that the said foreign Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) of the aforesaid section. The Controller has to record the reasons behind such revocation in writing and notify the same in the Official Gazette.[76]

2.8.1. Licence to Issue Electronic Signature Certificates

Section 21 of the IT Act, 2000 lays down the provisions for licence to issue Digital Signature Certificates. According to sub-section (1) of this section, any ordinary person may approach the controller with an application for the release of a licence so that he may be able to issue Digital Signature Certificate. But, such a

---

[75] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* pp.1024-1025 (Kamal Law House, Kolkata, 1st edn., 2008).

[76] Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.69 (Universal Law Publishing Co. Pvt. Ltd., 2nd edn., 2007).

licence may be given subject to the provisions of sub-section (2). And, in the sub-section (2), it has been provided that for the issuance of the licence by the Controller, there is a condition in which it is stated that the person approaching the Controller for the issuance of licence will have to fulfill such requirements just as qualification, expertise, man power, financial resources and other infrastructure facilities as are necessary for the issuance of Digital signature certificates. If he does not comply with these conditions, licence shall not be issued to him and what are the other infrastructure facilities, may be prescribed by the central Government. Sub-section (3) lays down the terms of a licence issued under the provisions of this section 21. It says that (a) a licence shall be valid for such period of time which may be prescribed by the central Government, (b) the license so granted shall not be transferred by anyone or it shall not be heritable; (the licence shall be governed by the provisions of the Information Technology (Certifying Authority) Rules, 2000 and the Information Technology (Certifying Authority) Regulations, 2001.[77]

2.8.2. Application for Licence

The Section 22 of the IT Act, 2000 prescribes the conditions for issue of a licence through filling an application in prescribed form.

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by a certificate practice statement;

(3) A statement including the procedures with respect to identification of the applicant

(4) Payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(5) Such other documents, as may be prescribed by the Central government.[78]

2.8.3. Renewal of Licence

An application for renewal of a licence shall be:

(a) In such form; and

---

[77] R.K. Chaubey, *op.cit.* p.1027.

[78] See, Sec. 22 of The Information Technology Act, 2000.

(b) Companied by such fees, not exceeding five thousand rupees, as may be proscribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.[79]

Rule 15 of the Information technology (Certifying Authorities) Rules, 2000 states that the provisions of Rule 8 to Rule 13 of the Information technology (Certifying Authorities) Rules, 2000, will apply in the case of an application renewal of a licence just as they apply to a fresh application for lie licensed certifying authority. Furthermore, the application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.[80]

2.8.4. Suspension of Licence

Section 25 of the IT Act, 2000 lays down grounds for the suspension of a licence. Sub-section (l) of Section provides that the Controller may revoke the licence, if, after making an inquiry, which he thinks proper, finds that a Certifying Authority has made a statement in relation to the application for the issue or renewal of the licence which is not correct or which is false in material particulars. Clause (b) of sub-section (1) of section 25 provides that if the Certifying Authority could not comply with the terms and conditions under which the licence has been given, the Controller have a power to cancel the licence. Clause (c) of this sub-section further provides that the licence may be cancelled by the Controller in that case also when the Certifying Authority does not comply with the procedures and standards which are provided under section 30.[81]

Section 25(1) in its clause (d) says that if the said Authority violates any provisions of this Act, rule, regulation or order made there under. However, in the proviso to this sub-section, it has been laid down that it is mandatory for the Controller to provide to the certifying authority a reasonable opportunity to show cause against the proposed revocation before his licence is revoked. Sub-section (2) of Section 25 lays down that if the Controller reasonably believes that there exists a ground for the revocation of a licence under the provisions of sub-section 1), he has a

---

79 See, Sec.23 of The Information Technology Act, 2000.
80 Vakul Sharma, *op.cit.*p.72.
81 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1030 (Kamal Law House, Kolkata, 1st edn., 2008).

right to pass an order to suspend the licence till the inquiry as directed by him is over. But, in the proviso to this sub-section, stress has been laid on the principle of natural justice. It says that the Controller shall give a reasonable opportunity to the Certifying Authority to defend himself against the proposed revocation. Sub-section (3) of this section imposes a bar on the Certifying Authority that he shall not issue any (electronic signature)[82] certificate during the period of the suspension of his licence.[83]

2.9. Duties of Subscribers

Every subscriber has been put under legal obligation to see that all representation made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true. Every subscriber is required to exercise reasonable care to retain control of private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber. The subscriber is under the statutory duty to communicate without any delay to the Certifying Authority if the private key corresponding to public key listed in the Digital Signature Certificate has been compromised. He is required to certify to all who reasonably rely on his information contained in the Digital Signature Certificate that he holds the private key corresponding to public key and is entitled to hold it, all representation made by him are true, and all information in the Digital Certificate that is within his knowledge is true.[84]

Chapter VIII of the IT Act, 2000 is about the duties of subscribers (Sections 40-42). The aforesaid Sections of the Act have to be understood along with the Information Technology (Certifying Authorities) rules, 2000 and Information Technology (Certifying Authorities) Regulations 2001 made there under. It is also important that due consideration should also be given to the Certification Policy Statement (CPS) of the licensed Certifying Authority.[85]

---

[82] Substituted by Information Technology (Amendment) Act, 2008 (10 of 2009), Sec. 2 for 'Digital Signatures' (w.e.f. 27-10-2009).

[83] R.K. Chaubey, *op.cit.*p.1030.

[84] B.R. Sharma, Runa Mehta "Information Technology Act, 2000: An Answer to 21st Century Legal Squabbles"38(1-4) *Civil and Military Law Journal* p.137 (2002)

[85] Vakul Sharma, *op.cit.*p.96.

2.9.1. Generating Key Pair

Section 40 lay down that the subscriber shall generate a key pair using a secure system. A key pair means a private key and its mathematically related public key, which are so related that the public key can verify a Digital Signature created by the private key. According to the provisions of this section, where a subscriber has accepted any Digital Signature Certificate, public key of which corresponds to the private key or that subscriber which is to be listed in the Digital signature certificate, the subscriber shall generate the key pair by the means of security procedure.[86] Generating a signing key pair (signing private/public key pair) is an important activity. It is imperative that private-public key pair shall be generated confidentially using the standards specified in the Act.

Rule 19(2) under the Information Technology (Certifying Authorities) Rules, 2000 establishes the 'Security Guidelines for Certifying Authorities'. As per para 18.1 of the said Guidelines:

(1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.
(2) The key generation process shall generate statistically random key values that are resistant to known attacks.

Furthermore, under the Regulation 4(1)(i) of Information Technology Certifying Authorities) Regulations, 2001 the subscribers are required to use private key/public key pairs that are 1024 bits long generated on a secure medium for purpose of signing. In addition, it is obligatory that before the generation of a Digital Signature Certificate by the Certifying Authority, the subscriber must generate a signing key pair successfully.[87]

2.9.2. Acceptance of Digital Signature Certificate

Section 41 of the IT Act, 2000 speaks about those conditions under which a subscriber shall be deemed to have accepted a Digital Signature Certificate. According to sub-section (1) of this Section, the condition for the acceptance of

---

[86] R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1046 (Kamal Law House, Kolkata, 1st edn., 2008).

[87] Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.97 (Universal Law Publishing Co. Pvt. Ltd. , 2nd Edn., 2007).

Digital Signature Certificate is that if a subscriber wishes his Digital Signature Certificate be accepted, he will have to publish or authorize the publication of a Digital Signature Certificate (a) to one or more persons; (b) in a repository; or otherwise shows his approval of the Digital Signature Certificate in any manner, only then he shall be deemed to have accepted a Digital Signature Certificate. As per sub-section (2) of it, emphasis has been laid on this fact that the Digital Signature Certificates help a lot in maintaining the trust in electronic medium. It says that by the acceptance of a Digital Signature Certificate, its subscriber certifies to all those persons, who have reasonable faith in the information contained in the Digital Signature, that the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same that all representations made by the subscriber to the certifying Authority and all material relevant to the information contained in the Digital Signature Certificate, are true and that all information in the Digital Signature Certificate that is within the knowledge of the subscriber, is true.[88]

A successful generation of a Digital Signature Certificate binds the key pair associate with the said Certificate to the subscriber (owner of the said certificate). But before the Certifying Authority issues the said Certificate to the subscriber, it shall have to obtain consent of the person (subscriber) to publish the said Certificate on a directory service (Rules 24 and 25). As mentioned in the aforesaid sub-section (1) acceptance of a Digital Signature Certificate is directly related to its publication, It has been provided under the rule 23(g)) that the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Digital Signature Certificate before he accepts it. It is further provided that upon acceptance of the issued Digital signature Certificate by the subscriber, the Certifying Authority shall publish signed copy of the Digital Signature Certificate in a repository (Rule 23(h)).[89]

2.9.3. Control of Private Key

Section 42(1) of the IT Act, 2000 speaks about the control of private key. According to it, the subscriber of the Digital Signature Certificate shall exercise all

---

88 R.K. Chaubey, *op.cit.*p. 1047.

89 Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.98 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

reasonable care to retain the control of the private key corresponding to the public key, which has been listed in his Digital Signature Certificate. This sub-section further says that the subscriber of such certificate shall try his level best to prevent its disclosure. He shall take all precautions so that its possible loss, disclosure to an unauthorized person and its misuse by such unwanted person should be checked. The Certifying Authority cannot be held liable for any such lapses. The subscriber is solely responsible for the protection of private key. According to the provisions of sub-section (2) of it, the whole force of a Digital Signature Certificate is on the integrity and confidentiality of the private key corresponding to the public key listed in the Digital Signature Certificate. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then the subscriber shall inform about it to the Certifying Authority as soon as possible ill the prescribed manner which may be specified by the regulations. In the Explanation to this sub-section (2), it has been clarified that for the purpose of removing the doubts, the subscriber of the Digital Signature Certificate must be held responsible till the time, the Certifying Authority is informed by him about the compromise of the private keys.[90]

The aforesaid sections 40-42 underline the duties of subscribers under the Act. By accepting a Certificate, the subscriber is bound by following obligations:

(a) Generating the key pair on a secure medium as specified in the Certifying Authority's Certification Policy Statement (CPS),
(b) Providing the correct information without any errors, omissions or misrepresentations in the application,
(c) Using the Certificate only for the authorized purposes as specified in the Certifying Authority's Certification Policy Statement,
(d) Demonstrate acceptance of the Digital Signature Certificate generated by the Certifying Authority when all information contained in the Digital Signature Certificate are as applied for and validated as true,
(e) Protecting the private key in a secure medium,
(f) Notifying immediately any change in the information included in the subscriber's Digital Signature Certificate that shall make the information in the Certificate inaccurate or misleading,

[90] R.K. Chaubey, *op.cit.*p.1048.

(g) Notifying immediately any suspected or actual compromise of the subscriber's private key, and

(h) Terminating the use of the Certificate if the information in the Certificate is found to be inaccurate and misleading.

Hence it is important that the subscriber should not only follow terms and conditions of 'Certifying Authority - Subscriber Agreement but also look for additional information as given in the Certifying Authority's Certification Policy Statement for better awareness.[91]

2.9.4. Electronic Signature

At the time of enactment, it has been felt that, as the internet being a public network so it would never be secure enough and there would always be a fear of interception, transmission errors, delays, deletion, authenticity or verification of an electronic message using internet as a medium. Hence, the goal was to protect the message, not the medium. The idea was to adopt a technology that makes communications or transactions legally binding. The functional equivalent approach extended notions of traditional paper-based requirements to a paperless world. That is, in order to be called legally binding all electronic communications or transactions must meet the fundamental requirements. In the first place authenticity of the sender to enable the recipient to determine who really sent the message, second message's integrity, the recipient must be able to determine whether or not the message received has been modified in the way or is incomplete and third, non-repudiation, the ability to ensure that the sender cannot falsely deny sending the message, nor falsely deny the contents of the message. It led to the acceptance of cryptography, a data encryption technique, which provided just that kind of message protection.[92]

Based on the nature and number of keys cryptography has evolved into symmetric and asymmetric cryptography. In symmetric cryptography, a single secret key is used for both encryption and decryption of a message, whereas in asymmetric cryptography encryption and decryption is done involving an asymmetric key pair consisting of a public and a private key.[93]

---

91 Vakul Sharma, *op.cit.*p.100.

92 R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* pp.998-999 (Kamal Law House, Kolkata, 1st edn., 2008).

93 *Ibid.*

The use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of encryption to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message. Generally, a Digital Signature is an appendage to its message and the transformations involved in creating the Digital Signature do not affect the message or make it confidential, although some implementations may provide for optional message confidentiality. Thus, contrary to cryptography used for confidentiality purposes, Digital Signature are annexed to the data and leave the content.[94]

Digital Signature are another form of security that the dual key technology offers. This digital signature is encrypted with a private key which when attached to a encrypted message uniquely identifies the sender. Since, the encryption used in the digital signature is linked to the message sent, 'forgers' would be unable to copy the digital signature by simply cutting and pasting it onto another message. The digital signature can also be combined with a digital time stamp to prove that the message was sent at a given time. A digital signature can be used as a' verification tool by anyone who has the user's public key. It is thus a method, whereby the recipient of the message can verify that the message did in fact come from the person who appended the signature to the message. Since, the signature uses the original text as an input to the encryption algorithm, the signature will not decrypt properly, if the message is altered in even the slightest way. As a result, the recipient can be sure that the message has been received unaltered and that the signature has not been copied from a different message. The reasons for placing a digital signature on an electronic document are the same as the reasons for placing a handwritten signature on a paper document.[95]

They are[96]:

- **Identification:** By placing a signature on a document, the signer identifies himself by the unique style of writing his name. Similarly, a digital signature uniquely identifies the sender of an electronic message.

---

94 Nandan Kamath , *Law Relating to Computers, Internet and E-Commerce* p.639 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

95 *Id.* at p.173.

96 *Id.* at p.174.

- **Authentication:** By performing the act of signing, the signer acknowledges that he authorizes and adopts the contents of the document. Similar intent can be attributed to the sender of the digitally signed email message.
- **Security:** A signature on a document should be difficult to forge. Moreover, some aspect of the signature, such as the individuality of the style of the person signing, offers security to the other party that as to the identity of the signer. Digital signatures offer the same form of security.
- **Tamper-resistance:** The nature of a written signature is such that changes to the signed text or the signature itself are clearly apparent except in the case of the cleverest forgeries. Digital signatures, if anything, is even more tamper-proof as they are almost incapable of being forged without actually altering the message irretrievably.

However, digital signatures are not perfect, since the efficacy of a digital signature is linked to the ability of the recipient to ensure the authenticity of the key used. Thus, if 'A' uses his private key to sign an otherwise unencrypted message, 'B' can verify that 'A' really sent it only if 'B' knows 'A's public key. In order to rely on the authenticity of that public key, however, 'B' needs to be assured of the authenticity of the key by some person other than 'A' sending the message, since if 'C' is forging a message from 'A' he will send his own public key as well, claiming that it actually belongs to 'A'. Since 'C' has the private key corresponding to the public key he sends 'B', 'B's attempt to verify the signature of the forged message will result in a confirmation of the message's authenticity, even though it is not really from 'A'. However, if 'B' is able to gain access to 'A' is real public key from some outside source; and uses it to verify the message signed with 'C's private key, the verification will fail, revealing the forgery.[97]

Thus, once again, if 'A' and 'B' are strangers with no alternate means of exchanging their public keys, no digital signatures or other cryptographic assistance, will reliably authenticate or identify them to each other. In USA, the state of Utah was the first jurisdiction to enact a Digital Signature Law,[98] recognizing the use of

---

97 *Ibid.*

98 The text of the Utah Digital Signature Act is *available at:*//www.jmls.cdu/cyber/ statutcs /udsa.html. (last visited on May13, 2013).

public key technologies and under which the rights and liabilities of the parties who use this technology, were established.

2.9.4.1. Functions of Signatures

Conventional handwritten signatures perform many functions. Electronic/digital signatures as 'functional equivalents' of conventional paper-based signatures should be able to achieve all of these functions[99]. In determining whether the security method used for an electronic signature is appropriate, legal, technical and commercial factors that may be taken into account include the following[100]:

- The sophistication of the equipment used by each of the parties;
- The nature of their trade activity;
- The frequency at which commercial transactions take place between the parties;
- The kind and size of the transaction;
- The function of signature requirements in a given statutory and regulatory environment;
- The capability of communication systems;
- Compliance with authentication procedures set forth by intermediaries;
- The range of authentication procedures made available by any intermediary;
- Compliance with trade customs and practice;
- The existence of insurance coverage mechanisms against unauthorized messages;
- The importance and the value of the information contained in the data message;
- The availability of alternative methods of identification and the cost of implementation;
- The degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
- Any other relevant factor.
- To identify a person;

---

[99] See, Sec. 5 of The Information Technology Act, 2000.
[100] See, Sec.16 of The Information Technology Act, 2000.

- To provide certainty and proof as to the personal involvement of that person in the act of signing;
- To associate the signer with the content of a document;
- As proof of the signer's intention that something has legal effect;
- To show the intent of a person to associate himself with the content of a document written by someone else;

2.9.4.2. Authentication of Electronic Records

Section 3 of the IT Act, 2000 lays down conditions under which a person, in whose name the digital signature certificate is issued, may authenticate an electronic record by means of his digital signature. A digital signature, according to "Webster's Universal Dictionary and Thesaurus", is an electronic version of a signature, which is encrypted and sent with a message, guaranteeing that the recipient gets a document that has not been opened by an unauthorized person. According to Section 2(l) (p) of the IT Act, 2000, 'digital signature' means an authentication of any electronic record by a subscriber by means of an electronic method on procedure in accordance with the provisions of Section 3 of IT Act, 2000. The digital signature consists of two distinct steps. At first step, the electronic record is converted into a message digest by means of a mathematical function which is known by the name of 'hash function' which digitally freezes the electronic record and hereby ensures the integrity of the contents of the desired communication or information consisting in the electronic record which is being so authenticated." If anyone tries to tamper with its contents, it shall at once make the digital signature invalid. [101]

In the second stage, the identity of the person, who affixes the digital signature, is authenticated by the use of a private key attaching itself to the message digest. The private key can be verified by anyone who is in the possession of the public key, which has similar position to that of private key. This will help anyone to find out as to whether the electronic record has been tampered with or not because it was so fixed with the digital signature. This will also help a lot to a person who has a public key to find out as to who is the originator of the message.

[101] R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1000 (Kamal Law House, Kolkata, 1st edn., 2008).

Section 3(2) of IT Act, 2000 provides that the authentication of the electronic record shall be put into effect by means of a system of a secure key pair which consists of a private key for creating a digital signature and public key to verify that digital signature which is, on the whole, given the name of 'asymmetric crypto system' (Section 2(1)(f) of IT Act, 2000) and 'hash function which envelops and transforms the initial electronic record into another electronic record. According to this sub-section, any subscriber may authenticate an electronic record by the use of his digital signature. In this, the source of an electronic record is determined, that is to say, the identity of the person, who has affixed his digital signature to authenticate any electronic record, is confirmed.

According to Section 2(1)(t) of IT Act, 2000, an electronic record includes data, record or data-generated image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche. In other words, any text, audio, video or multimedia content may be included in an electronic record. When the algorithm is executed with the name electronic record as its input, it produces the same hash result every time thereby it makes process of computing practicable. It may help in two ways - (a) to derive or reconstruct the original electronic record from the hash result which is produced by the algorithm; and (b) two electronic records can produce the same hash result using the algorithm.[102]

Sub-section (3) of this Section provides that the electronic record can be verified by any person by using public key of the subscriber. It means that a digital signature can be verified by any person other than the subscriber who has a public key. The verification of a digital signature has two functions. First, it verifies as to whether signer's private key was used to digitally sign the message. Secondly, it finds out as to whether the newly computed hash result tallies with the original hash result which has been derived from the digital signature during the verification process." According to sub-section (4) of section 3, the private key and public key, which are, of course, matchless, constitute a functioning key pair. According to Section 2(1)(zc), "private key" is the key of a key pair used to create a digital signature. As per Section 2 (l)(zd), "public key" is the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate. These two-private key and public key-make together a key pair. Section 2(1)(x) provides that in an asymmetric

[102] *Id.* at p.1001.

crypto system, key pair means a private key and its mathematically related public key which are so closely related that the public key can verify a digital signature created by the private key.[103]

2.9.4.2.1. Legal Recognition of Digital Signatures

Section 5 of the IT Act, 2000 where a law requires that information or any other matter shall be authenticated by adoption of any methodology or procedure used for the purpose or authenticating an electronic record by means of digital signature or any document shall be signed by any person. Then this requirement shall be deemed to have been fulfilled, provided such information or the matter is authenticated by affixing the digital signature in the method or procedure prescribed by the Central Government. According to Explanation attached to this section, the term signed, with reference to a person, means that any document shall be signed by such person under his hand or any mark on any document and expression signature shall be interpreted in the manner prescribed.[104]

2.9.4.2.2. The Technology for Electronic Signatures

The most common manner of signing electronically is with the help of public-key cryptography as contemplated by the IT Act, 2000. However, it must be remembered that there are other mechanisms as well. For example, certain techniques would rely on authentication through a bio-metrical device based on hand-written signatures. In such a device, the signer would sign manually, using a special pen, either on a computer screen or on a digital pad. The hand-written signature would then be analyzed by the computer and stored as a set of numerical values, which could be appended to a data message and displayed by the recipient for authentication purposes. Such an authentication system would presuppose that samples of the handwritten signature have been previously analyzed and stored by the biometrical device.[105]

---

[103] *Id.* at p.1002.
[104] *Id.* at p.1004.
[105] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.638 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

2.9.4.2.3. Public and Private Keys

Transaction security is a significant barrier to the development of E-Commerce. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. The most reliable means is through cryptography (i.e. encryption and decryption techniques). Cryptography uses sophisticated mathematical algorithms, particularly a technology known as '*asymmetric cryptography*'. Cryptography can be differentiated between the following:

- Use of cryptography for confidentiality of a message; and
- Use of cryptography in digital signature.

The most popular and useful method of encryption for general messaging is public key cryptography; that is, encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys, both of which are mathematically linked. One key is used for encryption and the other corresponding key is used for decryption. Each user has a pair of keys, of which the private key is kept secret and the public key is open to all.[106]

Before a sender can digitally sign an electronic communication, the sender must first create a public-private key pair.[107] The complementary keys used for digital signatures are termed

1. The 'private key', which is kept confidential to be used only by the signer to create the digital signature[108] and
2. The 'public key', which is ordinarily more widely known and is used by a relying party to verify the digital signature.[109]

A variety of methods is available for securing the private key. The safer methods store the private key in devices about the size of a credit card or $3^{1/2}$ inch floppy disk. Such a device or 'cryptographic token' executes the signature program within itself, so that the private key is never divulged outside the token and does not pass into the

---

[106] Subhajit Basu, Richard Jones, "E-Commerce and The Law: A Review of India's Information Technology Act, 2000" 12(1) *Contemporary South Asia* p.19 (March, 2003).
[107] See, Sec. 2(1)(x b) of the Information Technology Act, 2000.
[108] See, Sec. 2(1)(zc of the Information Technology Act, 2000.
[109] See, Sec. 2(1(zd of the Information Technology Act, 2000.

main memory or processor of the signer's computer. The signer must typically present to the token some authenticating information, such as a password; pass phrase, or personal identification number, for the token to run a process requiring access to the private key. Besides cryptographic tokens, other, generally less secure, methods exist for keeping the private key safe. Since, many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, for example by publication in an on-line repository on the internet or any other form of public directory where it is easily accessible.[110]

2.10. Legal Regulations of Cyber Appellate Tribunal (CAT)

The IT Act, 2000 establishes a judicial body to adjudicate upon matters arising within the Act called the Cyber Appellate Tribunal (hereinafter referred to as CAT). It is a fact-finding and as well an appellate authority. This is special judicial body meant solely to adjudicate upon the contraventions of the IT Act, 2000 and also to handle prosecution of the cybercrimes. This is a body, which acts like a court and has all the powers of a civil court established under the Civil Procedure Code, 1908 relating to calling of records, examination of witnesses, issuing summons and warrant, etc. Appeal is taken from the CAT to the High Court concerned and hence, the body sits between the adjudicating officer and the High Court. The cyber cases whether civil or criminal are new to the legal world and their area is also global hence, as many provisions of such laws are virgin, the CAT is a pioneer body and all its judgments and rulings would be a trendsetter. The main issues with which the CAT is required to deal with can be circumscribed as follows:

1. It deals with jurisdictional issues as the cybercrimes are global in nature and cannot be pinpointed to a single locality.
2. Being transborder crimes, there is bound to be a intermingling of various national laws in a single case or crime and hence, the CAT is also expected to look into the issues of private international laws.
3. The CAT is established especially for cyber activities whether concerned with online dealings or Electronic Commerce, or with violations of the IT Act, 2000 itself or with cybercrimes. Thus, the body is burdened with the responsibility of interpreting and evolving the provisions of cyber laws,

[110] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.640 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

intellectual property laws and traditional penal laws and as well as cybercrime specific laws.

4. The CAT is expected to face a challenge to strike a balance between the interests of the Government and end-users of the internet. It will help prevent all cyber contraventions and is destined to a path-breaking work to check cyber fraud, cybercrime and even cyber terrorism. [111]

Thus, the Tribunal will go a long way in paving the way for an easier, trustworthy and technology centric adjudication of legal provisions.

2.10.1. Cyber Appellate Tribunal after The IT (Amendment) Act, 2008.

Enormous changes have been made by the IT (Amendment) Act, 2008 in the matter of CATs. The erstwhile Cyber Regulations Appellate Tribunal (CRAT) has been replaced by the CATs. Chapter X containing Provisions regarding these Appellate Tribunals has been renamed as The Cyber Appellate Tribunal so also the word Regulations is dropped from Section 48. Sections 49-52 of the IT Act, 2000 have been replaced by a new set of sections. The changes mainly concentrate on techno legal nature of cybercrimes and have fulfilled the long awaiting requirement of including a technocrat in the Tribunal so that the legal provisions are interpreted with the help of technological expertise.

2.10.2. Establishment and Composition: New Changes

The CAT established under the amended Act will consist of:

1. One Chairperson-The Chairperson shall be appointed by the Central Government in consultation with the Chief Justice of India. A person to be appointed as the Chairperson must have the qualification to be a Judge of a High Court. (Sec. 50(1)) However, the amended Act says that the Presiding Officer appointed under the IT Act, 2000 would continue as the Chairperson of the present CAT. In the selection of the Chairperson and other Members of the Tribunal, the Central Government shall consult the Chief Justice of India (Sec. 49(2)).[112]

---

[111] Talat Fatima, *Cyber Crimes* p.474 (Eastern Book Company, 1st edn., 2011).

[112] Art. 217 of the Constitution of India, to be a Judge a person is required to have the following qualifications:

- He must be a citizen of India,
- He must have held a judicial office in the territory of India for a period of ten years, or

2. Other Members-Such number of other Members, as the Central Government may specify, would comprise the Tribunal. The Members shall be from the following fields:

(a) Technical Members-These Members are to be persons having special knowledge of and professional experience in information technology, telecommunication industry, and management or consumer affairs. They are to be appointed by the Central Government (Sec. 50(2)).

(b) Ordinary Members-The qualification of such Members include that he should be in the service of the Central or State Government and has held the post of Additional Secretary for a period of at least one year or the post of Joint Secretary to the Government of India or equivalent post in the Central or State Government for at least seven years (Sec. 50(2)).

(c) Judicial Members-The Judicial Members shall be appointed by the Central Government from persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for at least one year and a Grade I post of that for a period of at least five years (Sec. 50(3)).

3. The Chairperson and all the Members by virtue of Rule 12 of the CAT (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009 shall before entering upon the office would take oath of office and secrecy in Form I and II of the said Rules respectively.

4. Other Staff-The Central Government shall also appoint such officers and employees as it thinks fit to aid the Chairperson. This staff shall be under the general superintendence of the Chairperson and their salaries, allowances and other terms and conditions of service shall be prescribed by the Central Government (Sec. 56).

2.10.3. First Appeal: CAT

Within 45 days of the passing of the order of a Controller or of the adjudicating officer, the party may appeal to the CAT. The 45 days are counted from the day when the aggrieved person receives the copy of the order of the Controller or

---

- He has been for at least ten years an advocate of a High Court or of two or more courts in succession.
  In computing the period of ten years, the period in which the person has held an office of a member of a Tribunal or any post, under the Union or a State in which special knowledge of law is required is to be included.

the adjudicating officer when he can prefer an appeal. The appeal shall be in the prescribed form and accompanied with requisite amount of fee. The CAT may also consider an appeal even after the expiry of 45 days if sufficient cause is shown to it for the delay. After receiving the appeal, the Tribunal shall give opportunity to the parties for being heard, confirm, modify or set aside the order appealed against or pass such order as it thinks fit. The certified copy of such order shall be sent to the parties and to the Controller or adjudicating officer as the case may be. The CAT shall deal with the appeal as expeditiously as possible and every endeavour shall be made to dispose of the appeal finally within six months from the date of receipt of the appeal.[113]Section 57 makes provisions for an appeal to the Cyber Appellate Tribunal. According to them, person aggrieved by the order of an adjudicating officer has a right to make an appeal before the cyber Appellate Tribunal, which has the jurisdiction over the matter. Since, the right of appeal is the creature of a statute; therefore, an appeal may be preferred only when it is expressly provided for in the Act. An appeal has been defined as a proceeding undertaken to have a decision reconsidered by bringing it to a higher authority; specially the sub-mission of a lower court's or agency's decision to a higher court for review and possible reversal. According to longman advanced American Dictionary, an appeal is a formal request to a court or someone in authority asking for a decision to be changed.

According to sub-section (2) of this Section, if an order has been made by an adjudication officer with the consent of the parties, then no appeal shall be preferred to the cyber Appellate Tribunal. Consent between the contesting parties denotes a compromise or settlement. According to the 'Oxford Companion to Law', consent always implies freedom of judgment, deliberations and freely given acquiescence in what is considered desirable. There is free consent only if the person is not blinded by anger or intoxicated, or ignorant or deceived subject to duress or over reached. As per sub-section (3) of the Section, an appeal may be preferred before the cyber Appellate Tribunal by a person, who is aggrieved by the order of the controller as the adjudicating officer, within 45 days from the date of receipt of the order by the person so aggrieved. A prescribed fee in this regard shall accompany the form of appeal. Proviso to this sub-section lays down the terms for the condonation of delay in filing an appeal after the period aforesaid. The proviso says that the cyber Appellate

[113] Talat Fatima, *Cyber Crimes* p.481 (Eastern Book Company, 1st edn., 2011).

Tribunal may entertain an appeal after the expiry of the said period of 45 days if it is satisfied that there was 'sufficient cause' for not filing it within that period.[114]

Sub-section (4) lays down that when an appeal under sub-section (1) is received by the cyber Appellate Tribunal, it shall give an opportunity of being heard to the parties to appeal. After hearing both the parties, it may pass such orders, which it deems proper. While passing the orders, it may either confirm the order against which the appeal has been made, or modify it or set it aside. According to sub-section (5), the Cyber Appellate Tribunal shall send a copy of every order passed by it to the parties to the appeal and to the concerned controller or adjudicating officer. The word 'shall' used in this sub-section denotes that it is mandatory for him to communicate the order passed by it to the parties and officers concerned, and the contesting parties are entitled to a copy thereof. As per the provisions of sub-section (6), an appeal under sub-section (1) filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible. It is heartening to note that it has set a time period of six months to finally dispose of the appeal. This period shall commence from the date of receiving the appeal.[115]

2.10.4. Power and Procedure of the Cyber Appellate Tribunal

The Cyber Appellate Tribunal (hereinafter referred to as CAT) is the judicial body established under the Act. It is a specialized body, which looks into the contraventions of the IT Act, 2000 and serves as the court of first appeal. It is the lowest judicial body from where appeal is taken to the High Court concerned. The Act itself lays down the procedure of the Tribunal and excludes the bondage of the Tribunal to the provisions of the Civil Procedure Code, 1908 (5 of 1908). The CAT shall have the same powers as are vested in a Civil Court under the Civil Procedure Code, 1908 (5 of I908) as follows: (Sec. 58(2))

1. Summoning and examining any person on oath;
2. Requiring the discovery and production of documents or electronic records;
3. Receiving evidence on affidavit;
4. Issuing commissions for the examination of witnesses or documents;

---

[114] R.K. Chaubey, *op.cit.*p.1071.
[115] *Id.* at p.1073.

5. Reviewing its decisions;
6. Dismissing an application for default or deciding it ex parte; and
7. Any other matter, which may be prescribed. [116]

Thus, the CAT has been given elaborate powers to deal with the situations arising out of electronic activities online and with Contraventions of the IT Act, 2000 itself.

2.10.4.1. Procedure

The CAT shall be guided by the following principles in its working:

1. Rules of natural justice;
2. By the related provisions of the IT Act, 2000; and
3. By the CAT Rules, 2000.

Thus, Section 58 of the IT Act, 2000 empowers the Tribunal to lay down not only its own procedure but to also decide the place of its sitting. The Tribunal is free to apply the well-settled rules of Natural Justice, which are as follows:

2.10.4.1.1. The Doctrine of Bias

This rule says that no one shall be a Judge in his own cause. This upholds the concepts of impartiality and fairness and says that the Presiding Officer shall be free from any prejudices. The Supreme Court held in *C. Sarana* v. *University of Lucknow*[117] that the authority to decide the dispute between Opposing parties must be one without bias. This rule of bias is only a principle of conduct and is imposed strictly on the exercise of the judicial or quasi-judicial authorities. In case of bias, the actual proof is not necessary.[118] The real likelihood of bias is necessary and the test is that of a reasonable man.

2.10.4.1.2. Audi Altarem Partem

It is another rule of natural justice, which implies the right to be heard. The rule has two facets; notice of the case to be met and opportunity to explain. Justice cannot be done unless both the sides are given the opportunity to explain their

---

[116] Talat Fatima, *Cyber Crimes* p.482 (Eastern Book Company, 1st edn., 2011).
[117] AIR 1967 SC 2428.
[118] U.P.D. Kesari, *The Administrative Law* p.161 (Central Law Publications,1st edn., 2003).

situations and to use the words of Lord Loreburns, it is "*a duty lying upon everyone who decides something*" in the exercise of legal power. This rule cannot be ignored for the sake of the convenience of the authority as Lord Atkin rightly says "*convenience and justice are often not on speaking terms*". Thus, even though some delay, inconvenience or hardship be suffered by the authority or by anyone, the incriminating material is made known to the accused and he should be given an opportunity to defend himself.[119]

2.10.4.2. Real Justice

There is often one more accepted rule of natural justice which says that justice should not only be done but it should be done in such a material manner that one should feel that justice has been done. In other words, justice should not be an artificial thing only by way of pretension or show but it should be actually done so that the aggrieved feels that justice has been met. The IT Act, 2000, wherever Possible, has also mentioned certain rules, which are to be followed by the Tribunal. These facets of procedure before a Tribunal are retrieved from the following sections of the Act:

(a) Limitation

The appeal to be filed before the Tribunal must follow the period of limitation for filing a suit. This is done on the basis of the provisions of the Limitation Act, I963 (36 of 1963) (Sec. 60 of the IT Act, 2000).

(b) Jurisdiction

By virtue of Section 61, the IT Act, 2000 ousts the jurisdiction of a civil court. Such prohibition is regarding two things; firstly no civil court shall have jurisdiction to hear any suit or proceedings in respect of any matter which an adjudicating officer appointed under this Act or the CAT is already empowered to determine and secondly, no injunction can be granted by any court or authority regarding any action taken by such officer or Tribunal.

(c) Representation

The appellant has been given option to either plead his appeal personally or he can also take the help and advice of the legal practitioners of his choice (Sec. 59).

[119] Talat Fatima, *op.cit*.p. 483.

Thus, the Act also provides for some part of the procedure to be followed by the Tribunal. Section 58 also declares that the procedure shall be subject to the rules made by the Central Government. Thus, in exercise of powers conferred by Section 87 of the IT Act, 2000, the Central Government made the rules called the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 (Rules, 2000). The Rules, 2000 has 28 rules which detail out the procedure of filing the application, the procedure of filing the reply and other appeal related procedures.[120]

2.10.4.3. Procedure for Filing the Application

The appellant shall file the application in the Form I annexed to the Rules, 2000 either in person or through his agent or lawyer (Rule 3). It can also be sent by registered post addressed to the Registrar (Rule 5). Such application shall be presented in six complete sets in a paper book form and if there is more than one defendant then required number of paper-books along with empty envelopes bearing the address of the defendants should also be filed. An acknowledgement receipt may also be attached. The paper-book shall also be accompanied by a certified copy of the impugned order, copies of documents on which the party relies its stand attested by an advocate, and if it is being filed by an advocate then it shall also be accompanied by the 'Vakalatnama'[121] (Rule 8).

However, the Tribunal can also allow single application to be filed when there are more than one person if they have the same interest in the service matter, and where there is an association and more than one persons are interested in joining in a single application then the Tribunal may also allow them, provided all give their personal details in the application (Rule 3). On presenting the application, the Registrar shall after scrutinizing the application and finding it in order shall register it and give a serial number to it. On finding a defect, the Registrar shall ask the applicant to remove the defect and if he fails to do so, the Registrar shall have power to decline to register the application. The applicant, on such declining to register the application, can make an appeal to the Tribunal within 15 days of its rejection (Rule 4). The application shall also be accompanied by a fee of Rs 2,000 as application fee (Rule 6). An application based upon a single cause of action may plead for more than

[120] *Id. at* p. 484.

[121] A vakalatnama is a document which is the authority given by the client to the lawyer to plead his case in the law court. It is signed both by the lawyer and the client. It is a kind of proof of contract between the lawyer and his client.

one remedy if they are consequential to one another (Rule 9). The application shall be drafted in paras well numbered mentioning the grounds for such application under distinct heads. Such application may also contain a prayer seeking an interim order or direction pending final disposal of the application, or it may also after filing an application under Section 57 of the IT Act, 2000 apply for an interim order or direction.[122]

2.10.4.3.1. Service of Notice

After duly accepting the application, the Registrar shall then serve a copy of the application in the paper-book to each of the respondents either by hand delivery, through the applicant, through a process server or through registered post with acknowledgement due. The Registrar can also use any other manner including the manner of substituted service which appears to him just and convenient to serve the notice. If the number of respondents exceeds five then the applicant shall have to pay a sum of Rs 50 for each of the service to respondents. The Tribunal can also exercise its discretion to go ahead with the hearing even though the notice has not been served to certain respondents and the Tribunal is of the opinion that the interest of the respondents to whom notice has not been served has been adequately represented by the applicant. It shall record the reasons for doing so. However, the Tribunal shall not proceed with the hearing unless it has served notice upon the government or on the authority which passed the impugned order (Rule 10).[123]

2.10.4.3.2. Procedure for Filing The Reply

Within one month of the receipt of the notice, the respondent shall file the reply in six sets along with the documents in a paper-book form with the Registrar. The respondent shall also send a copy of the reply to his advocate and the proof of such service shall be sent to the Registrar (Rule II).[124]

2.10.4.3.3. Disposal of Application

Once the above procedure is done, the Tribunal shall notify the date and place of hearing to the parties (Rule 12). The Tribunal shall draw up a calendar for the hearing of the transferred cases and should follow the calendar strictly. Every

---

[122] Talat Fatima, *op.cit*.p.485.
[123] *Ibid.*
[124] *Ibid.*

application shall be heard and disposed of within six months of its presentation. The Tribunal shall have power to decline and adjourn and to limit the time for oral argument (Rule 14). In case the applicant does not appear on the date of hearing, the Tribunal shall have power to dismiss the application for default or hear and decide it on merit. In case after the dismissal the applicant appears and satisfies the court regarding his absence then the court may set aside the order and hear the case anew (Rule 15).

In case the respondent is absent on the date of hearing, the Tribunal using his own discretion either adjourn or dispose of the application ex parte. If, thereafter, the respondent appears and applies to set aside the ex parte order saying that his non-appearance was due to some irregularity in serving the notice or for some other sufficient reason and the Tribunal is satisfied then it will set aside the ex parte order and proceed with the application. But if the Tribunal is satisfied that in spite of the irregularity in service, the respondent had sufficient time to appear then it will not set aside the ex parte order (Rule 16). The order passed by the Tribunal shall be signed by the Presiding Officer and date will also be given (Rule 17). Every such order shall be sent to the applicant and to the respondent free of cost by registered post (Rule 20).[125]

2.10.4.4. Second Appeal: High Court

From any decision or order of the CAT, the aggrieved may file an appeal before the High Court. Such appeal has to be preferred within 60 days of the communication of the decision or order of the CAT to the aggrieved party. The appeal can be on any question of fact or law arising out of such order. However, on the expiry of the said 60 days, the High Court can accept the appeal within another 60 days if it is satisfied that the appellant was prevented by sufficient cause to make an appeal within time (Sec. 62).[126]

2.10.4.5. Compounding of Contraventions

The IT Act, 2000 provides for the compounding of contraventions before or after the institution of adjudicating proceedings. The contravention can be compounded by the Controller or the adjudicating officer subject to such conditions as

[125] Talat Fatima, *Cyber Crimes* p.486 (Eastern Book Company, 1st edn., 2011).
[126] *Ibid.*

specified by such officer. The compounding sum shall not exceed in any case the maximum amount of the penalty provided for such contravention. Such compounding shall not be allowed to the person who commits contraventions within three years of compounding of any contravention. Nevertheless, a contravention after the expiry of the said period of three years shall be deemed to be the first contravention. After compounding of any contravention, no proceedings against such person guilty of the compounded contravention shall be taken (Sec. 63). Any penalty unpaid or compensation awarded shall be recovered by the Controller or the adjudicating officer as the arrear of land revenue and the licence or the Electronic Signature Certificate, as the case may be shall be suspended till the penalty is paid (Sec. 64, Amended 2008).[127]

2.11. Information Technology Act, 2000: Regulation and Liability of Network Service Providers

A network service provider represents an interactive network service. It may provide access to the internet (network of networks) only or offer a range of additional resources. Depending upon its functional attributes a network service provider may act as an information carrier or information publisher. A network service provider is also an important link to the World Wide Web as it not only transmits, distributes or publishes but also helps in creating an Interactive wired world. It is thus necessary that the liability, if any, of network service providers be seen by understanding their nature of work and the degree of limitation on account of technological advancement. A network service provider means any person who provides access to information service in electronic form. The examples are Internet Service Providers (ISPs), cellular mobile services, customer access services (call centers), mobile satellite services, bandwidth services, cable operators, etc[128]

It must be noted however that this provision operates in the form of a reverse onus clause where the duty is cast on the ISP to prove that he had no knowledge of

---

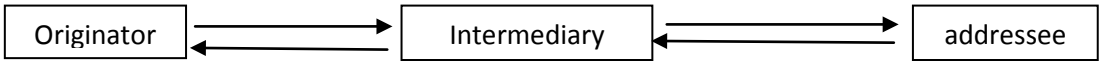
[127] *Id.* at p.487.

[128] Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.186 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

the existence of the materials and that he had exercised all due diligence to prevent the commission of the offence.[129]

In this case, *Sanjay Kumar Kedia* v. *Narcotics Control Bureau and Anr.*[130] Supreme Court observed that Special Leave was granted and a Division Bench issued Notice on the Special Leave Petition noticing a contention raised by Mr. Tulsi that service providers such as the two companies, which were intermediaries, were protected from prosecution by Section 79 of the Information Technology Act, 2000. An affidavit in reply has also been filed on behalf of the respondent - Narcotics Control Bureau and a rejoinder affidavit in reply thereto by the appellant. It was held that Court shall not release accused on bail, unless reasonable ground is established.

Primarily, a network service provider is to perform two tasks: (a) to provide access to the network and (b) to act as an Intermediary[131] with respect to any particular electronic message. The function of a network service provider has to be understood in the terms of its role as a facilitator with respect to any particular electronic message between an originator and an addressee.[132]



Network Service Providers as an Intermediary

2.11.1.1. Network Access Service Provider

The primary function of a network service provider is to provide access to the network. This could be in the form of dial-up, broadband, satellite, microwave or any other communication media. In order to provide such 'network' connectivity, the

---

129 Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* pp.664 -665 (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000).

130 MANU/SC/8158/2007.

131 Under the Act an "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message (5. 2(1) (w) of The Information Technology Act, 2000).

132 Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.186 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

network service provider needs to have information technology infrastructure in place.[133]

2.11.1.2. Network Intermediary

Network service provider is to act as an intermediary between the originator and the addressee. It does not mean that all intermediaries are network service providers. For example, a search engine though may be referred as an intermediary but it is not a network service provider. [134]In the context of internet, an act of publication includes distribution also. The question is, under what circumstances[135], would a network service provider (ISP) be held liable?

(a) The ISP knows, or has reason to believe, that the information content it is transmitting is unlawful.

(b) Regardless of the ISP's knowledge, it benefits directly from the transmission (i.e. it receives benefits beyond the indirect benefit that it receives from internet access fees).

(c) The ISP fails to take reasonable steps to determine if the information content that it transmits is unlawful.

On one hand, mere knowledge of unlawful content makes them liable and on the other, it is technologically infeasible to act on or take cognizance of a 'real time' offence or contravention and initiate a preventive action accordingly. Hence, it would be prudent if ISPs models were not judged from physical world legal liability requirements.[136]

2.11.2. Network Service Providers Not to be Liable in Certain Cases

Section 79[137] of the IT Act, 2000 enumerates certain cases when network service providers are not liable. It removes doubts and makes it clear that if any

---

133 *Id.at* p.187.

134 *Ibid*.

135 E.D. Reed Chris, Angel John, *Computer Law* p.390 (Universal Law Publishing, Indian Reprint, 4th edn., 2002).

136 Vakul Sharma, *op.cit.* pp. 188-189.

137 See, Sec. 79 of The Information Technology Act, 2000, Network service providers not to be liable in certain cases. For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed

person proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention, he shall not be punished under this Act, rules or regulations made there under for any third party information or data made available by him.[138]

The aforesaid section expresses the legislative intent of granting immunity to the network service provider. The said immunity is absolute if and only if he proves for any third party information that:

(i) He had no knowledge that the information content it is transmitting is unlawful; or

(ii) He had exercised all due diligence to prevent transmission (or publication) of unlawful information content. No immunity is available if it is transmitting or publishing proprietary content. Interpretation of the words 'knowledge' and 'due diligence' is crucial for the understanding and application of this section.[139]

In this section, two things are important ‘Knowledge’ and ‘due diligence’. So for as Knowledge, according to Black's Law Dictionary,[140] are of mainly two kinds: (i) actual knowledge which means direct and clear knowledge, as. Distinguished from constructive knowledge; (ii) constructive knowledge, which means knowledge that one using reasonable care or diligence, should have, and, therefore that is attributed by law to a given person.[141]Knowledge means actual or constructive knowledge, i.e. a person is deemed to have constructive knowledge of the contents of material, which would put a reasonable and prudent person on notice as to the suspect nature of the material. That is, the network service provider knows, or has reason to believe, that the information content it is transmitting is unlawful.[142]

---

without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention,

138 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1096 (Kamal Law House, Kolkata, 1st edn., 2008).

139 Vakul Sharma, *Information Technology : Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* pp.188-189 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

140 Bryan A Garner, *The Black's Law Dictionary* (7th edn., 1996).

141 R.K. Chaubey, *op.cit.* p. 1098.

142 Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.193 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

Due diligence means reasonable steps taken by a person in order to avoid commission of offence or contravention, i.e. adopting reasonable steps to determine if the information content it transmits is unlawful. A due diligence exercise is a statutory duty on the part of the network service provider to have regulatory practices to prevent transmission or publication of the unlawful content. For example, a service provider, who provides any service to the 'third parties', may be held liable if he fails to block the access to the harmful content despite the fact that it is technically possible to block the said access.[143] The explanation third party information means any information dealt with by a network service provider in his capacity as an intermediary. The dictionary meaning of third party means a person or group besides the two primarily involved in a situation. In terms of "third party information, it would mean information generated by a person or group besides the two primarily involved in information generation. It implies the information resources generated by an independent person or group. In the context of this section third party information would mean the information received, stored or transmitted by the network service provider as an intermediary from independent person or group.

In this case, *Ratan N. Tata* v. *Union of India (UOI) and Ors.*[144] Supreme court observed that Issue a writ order or direction under Article 32 of the Constitution directing the Respondents, their servants and agents to ensure that no further publication of these recordings-either as audio files through the internet or any print as transcripts appears in any media-print or electronic and for that purpose, take steps as may be necessary, including but not limiting to steps under The Cable Television Networks (Regulation) Act, 1995 and The Information Technology Act, 2000, the Code of Criminal Procedure, 1973 read with the Indian Penal Code, 1860 and any other law, as may be necessary.

In a way, the aforesaid section of the Act is consistent with the statutory provisions prevailing in other countries. This section should not be viewed and applied in isolation but always in reference to the offence or contravention committed. Furthermore, it calls for adoption of flexible approach on the part of the judges to

[143] Vakul Sharma, *op.cit.* p.192.
[144] MANU /SC/1090/2013.

address the legislative intent behind the provision rather than to make the network service provider liable on non-existent issues.[145]

2.12. Information Technology (Amendment) Act, 2008

The Government of India has brought major amendments to IT Act, 2000 in form of the Information Technology Amendment Act, 2008. The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed on 23rd December 2008 and received the assent of President of India on 5th February, 2009. The IT Act 2008 has been notified on Oct. 27, 2009. Though, the IT Act, 2000 technically became law of the land, yet it did not come into operation as Section 1 (3) of the said Act specifically stipulated that it shall come into force on such date as the Government may, by notification, appoint. [146]

The IT Act, 2000 aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'Electronic Commerce', which involve the use of alternatives to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the government agencies. In addition, the Central Government also notified two distinct kinds of Rules. These rules are The Information Technology (Certifying Authorities) Rules, 2000 and the cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. The Information Technology (Certifying Authorities) Rules, 2000 detail various aspects and issues concerning to Certification Authorities for digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures. The said rules also stipulate security guidelines for certification authorities and maintenance of mandatory databases by the said certification authorities and the generation, issue, tern and revocation of digital signature certificates. [147]

---

[145] Vakul Sharma, *Information Technology: Law and Practice; Law and Emerging Technology Cyber Law and E-Commerce* p.192 (Universal Law Publishing Co. Pvt. Ltd. , 2nd edn., 2007).

[146] Sujeet Kumar, *Encyclopaedia of Cyber Laws* p.231 (ABD Publishers, New Delhi, 1st edn., 2011).

[147] *Id.* at p.232.

The overall net affects of all these notifications are that the IT Act, 2000,has come into operation. The information in the electronic format has been granted legal validity and sanction; digital signatures have been defined and made legal. It is now possible to retain information in an electronic format. Electronic Contract has been recognized to be legal and binding. Some types of cyber crimes have been defined and made punishable offences like hacking, damage to computer source code, publishing of information, which is obscene in the electronic form, breach of confidentiality and privacy and publishing digital signature certificate false in certain particulars and for fraudulent purpose.[148]

The lacunae in the IT Act, 2000 for long necessitated a refurbishing of the legislation. This was achieved in 2008 when the Act is not only thoroughly amended but a lot more is done. The lone cyber Act was technology centric, which is why not much attention is given to the commerce or economy in this amendment. The loud and clear message is that the Government has awakened to the importance of cybercrimes and has realized the magnitude of hazard. It can pose to the security of the country.[149]

The amendment was passed in an eventful Parliamentary session on 23rd of December 2008with no discussion in the House. Some of the cyber law observers have criticized the amendments on the ground of lack of legal and procedural safeguards to prevent violation of civil liberties of Indians. There have also been appreciation about the amendments from many observers because it addresses the issue of Cyber Security. Section 69 empowers the Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.

---

[148] *Id.* at p.233.

[149] Talat Fatima, *Cyber Crimes* p.498 (Eastern Book Company, 1st edn., 2011).

2.12.1. Information Technology Act, 2008: Some Important Highlights

The amendment though extensive is at the same time a positive step to bring the cybercrimes within the legal net. A glance at the changes gives the following headlines: [150]

1. The most prominent change is the replacement of the term 'Digital Signature' by the term 'Electronic Signature' thus making the law more technology neutral, which has been the approach of the Model Law on Electronic Signatures, 2001.
2. It can be said without doubt that major amendments have been in the long awaited criminal area. A host of new cybercrimes like child pornography, obscenity, depiction of sex explicit act, violation of privacy, cheating by personation, identity theft, cyber terrorism, sending offensive messages, have been introduced.
3. Offences under the Act are categorized into bailable and cognizable which has been done for the first time under the Act. This will give the police more freedom to act.
4. Attempts and abetments of offences is also recognized as an offence under the Act.
5. The amendments are more investigation friendly and are paving the way for a more fruitful and easier way to investigate cybercrimes and other online illegal activities. The complaints regarding these offences can now be looked into by an officer of the rank of Inspector and the earlier provision for Deputy Superintendent of Police has been done away with.
6. Terms like 'cyber cafe', 'e-mail', 'communication device' have been defined. This has enlarged the area of law and has enriched its language to meet the internet situations.
7. Cyber security has been addressed well. Elaborate provisions are introduced to safeguard cyber infrastructure in the country. For this, provision for the establishment of a National Nodal Agency (ICERT) has been introduced.

---

[150] *Ibid.*

8. The term ‘intermediaries’ has been defined to include within its area a number of other service providers so as to enlarge the liability susceptible class in cyberspace.
9. National security has been given an upper hand. For this, monitoring, intercepting and decryption of flowing information has been made mandatory by the intermediaries and any person in charge of a computer source on the directions of proposed governmental agency. Failure to follow the directions has been made an offence.
10. The judicial regime under the Act has not only been fortified with more Members but it is made more specialized and purposive by inducting technocrat in it, thus realizing the technological nature of cybercrimes.
11. To make the evidence more acceptable and reliable, the report of the Electronic Evidence Expert has been made relevant under the evidence law by making an amendment under the same.
12. Law weds technology as in the number of new and amended sections; it is made obvious that without technological expertise and the digitization of the legal process little can be done to counteract the silicon onslaught.

As the law relating to cybercrimes is in its infancy. Hence, there is a lot more scope to develop the legal provisions. From a rural and agriculture dominated entity, India has travelled a long journey on the Information Superhighway, and today can boast of being an Information Superpower. The communicational developments are flourishing well, and with it, the computer criminal is making headway. All this necessitated the establishment of an effective and technology-centric law and enforcement regime. With that, in view the amendments make a positive headway to meet the legal exigencies. About more than two dozen new provisions have been added to cover the situations, which were left out by the IT Act in 2000.[151]

Conclusion

The IT Act, 2000 was drafted on the base UNCITRAL MODEL LAW on the Electronic Commerce adopted in 1996. In the IT Act, 2000, not only provisions relating to E-Commerce but also Computer Crimes and offences along with

[151] Talat Fatima, *Cyber Crimes* pp.499-500 (Eastern Book Company, 1st edn., 2011).

punishment have been mentioned and well defined. Moreover, the powers of the police to investigate, search and seize have also been specified. It is important to mention that IT Act, 2000 encompasses not only E-Commerce but also something more like Computer Crimes and amendments to the Indian Penal Code. In other words, it can be said that it covers more issues relating to cyber world than UNCITRAL Model Law. The main purpose behind this was to facilitate E-Commerce transaction and its smooth functioning. This step in the IT Act, 2000 is welcome as it will have a instructive effect. The Information Technology Act is a praiseworthy piece of legislation in India dealing with E-Commerce and other related aspects. It is based on the spirit of the UNCITRAL Model law on E-Commerce. However, it should be kept in mind that the Model law was not intended to cover every aspect of the use of Electronic Commerce. It is, therefore, many more substantive areas that need to be addressed suppose consumer protection, data protection, spamming, intellectual property, etc.

There should have separate legislation for some of the above rather than complicating the IT Act, 2000 with numerous things. Similarly, though the provision relating to electronic signatures suited the country's prevailing circumstances and available technology at the time of passing the legislation, it must be amended with the course of time in order to accommodate changing technological advances. As business activates by the electronic means are increasing, it has become very important that evidence of these activities should available to demonstrate legal rights and obligations that flow from them. India has become among the first few countries, which have passed a separate comprehensive law regulating E-Commerce and other IT enabled services. But there are still many important issues of E-Commerce (e.g. Intellectual Property Rights, data Protection, Domain Names Disputes, Electronic Payment System, Data Protection, Protection of Consumers, Privacy and E-Taxation), which are important for the development of this new technology, but has not covered by the IT Act, 2000. Added to these issues, the Act does not properly deal over complex provisions relating to contract formation the ties to particular technology in the regulation of digital signatures, the over elaborate mechanisms for controlling certification authorities and the attempts to define the technology stand in stark contrast to more minimalist approaches adopted in other jurisdictions.

The IT Act, 2000 as a cyber specific legislation in the field of E-Commerce was essential for proper and smooth governance of the new technology. Without a new set of laws of governance, the new society that had sprung up suddenly due to the new technology could not function properly. The new environment, therefore, requires new set of laws may also be mentioned that the internet is being increasingly used for pornography, gambling, trafficking in human organs and prohibited drug, hacking, infringing copyright's and violating individual privacy etc. Therefore, it was needed that the law should regulate the human activities in cyber space and fill up the gap of law in the field of E-Commerce. E-Commerce systems operating over open systems such as the internet can also be operated outside geographical boundaries. Within India, this creates important questions relating to the applicability of the state laws to transactions that may be initiated by a consumer in one state who uses a financial institution headquartered in a second state to make payments to recipients located in other states, by means of a computer at some unknown location. These challenges are even greater at the international level. While the IT Act, 2000, deals with the domestic legal issues, nation-states may find unilateral enforcement of E-Commerce related rules.

Crime does not know frontiers and the criminal has no sense of patriotism, humanism or jurisprudence. However, the crime of the modern age has become borderless; the accusatorial laws would have to take international character. In the present Global era, on the one hand, it is good for having the information technology and its advancement the legal fraternity, it is a challenging. A new legal infrastructure partaking of both the time-tested penal laws as well as the newly made cyber laws of the legally developed systems would go a long way in giving a tough resistance to the cyber onslaught. India is moving steadily on the path of cyber legislative activity and the country has established itself as the Information Superpower and with the amendment in 2008 in the cyber law, it has made a meaningful effort to address the amazing challenges of the information society but still so little has been achieved so much yet to do. The unyielding technology and the weary law would be in conflict for some more time. This Act is the over complex provisions relating to contract formation the over-elaborate mechanisms for controlling certification authorities and the attempts to define the technology stand in stark contrast to more minimalist approaches adopted in other

jurisdictions. In essence, the effect of the Information and Technology Act is quite significant because of information and communication revolution in India as well as in other countries of the world at large. Honestly, the IT Act, 2000 has addressed to a considerable extent the legal questions involved in adopting the Cyber Medium for Communication, Contract and Commerce.

CHAPTER III

ELECTRONIC CONTRACT UNDER DIGITAL TECHNOLOGY

Introduction

The World Wide Web (WWW) is new digital technology which has brought new opportunities and imposed challenges to existing legal environment. The corporate business explores and utilizes it for their benefit by expanding their activities not only in physical space but also in virtual space in search of the potential customers. While E-Contract has become a fundamental element in the E-Commerce world, the Electronic Contract raises various new legal issues. Generally, the legislature and the legal profession inclines to apply the existing law to the new sets of virtual commerce problems without much change and modification is necessary or unavoidable to protect the interest of e-businesses and e-consumers. Before understanding Electronic Contracts, it is essential to understand the general principles of contract and the law governing contracts in Indian perspective. Contract is always an essence in the agreement between two or more parties to conduct any business transaction. Such a contract must be valid and legally binding on the parties to be made mutually benefit their interest and transactions. These contracts may be oral or written as may be required by law in specific cases and is validated by the law.

In any community settings, breach of contract is settled through community adjudication legal system, which inquired into the breach and set right things. As with the evolution of the legal system, contracts came to be governed by specific laws under the respective legal systems. In other words, a contract is an agreement for a specified transaction between two or more parties for a specified consideration and is binding upon the transacting parties. The Contract, oral or written, is made through a process of negotiation with offers/proposals, counter offer/counter proposals towards acceptance by the contracting parties. Such an acceptance turns into an agreement. The Section 2(h) of the Indian Contract Act, 1872 clearly states that an agreement enforceable by law is a contract.

The internet has unfolded a new market for businesses to explore and exploit. It is to provide security and legal recognition to the transactions executed

electronically. Indian Parliament has enacted The Information Technology Act, 2000 (hereinafter referred to as the IT Act, 2000) which has come into force on October 17th, 2000. This Act modelled on the United Nations Commission on International Trade Law (UNCITRAL) Model Law, but departs in many respects from the spirit of the Model Law. Furthermore, the Indian courts could not yet found any opportunity to appraise the impact of the provisions of the IT Act, 2000 on substantive principles of contract formation codified in The Indian Contract Act, 1872. Immediately after the enactment of the IT Act, 2000, it was felt that certain significant provisions were missing in this enactment and its provisions lacked harmony and above all many legal issues had not been properly spelled out. This Act was amended in the year 2008 with several objectives. An attempt is made in this chapter to analyze the legal provisions relating to E-Commerce in the IT Act, 2000 together with the provisions of The Indian Contract Act, which continues to be the fundamental law on the subject. Hence, an analytical evaluation should be made to identify the issues raised by the information technology relating to contract formation and impact of the IT Act, 2000 on the basic principles relating to contract formation provided in the Contract Act, impact of non inclusion of the principles governing E-Commerce, provided in the Model Law but not reflected in the IT Act, 2000 and the jurisdictional issues which are not confined to national boundaries.

The present millennium is witnessing a new culture, internet culture, which will change our way of life. In the beginning, it was confined to military establishments but the internet has, due to its speed, interactivity and flexibility, tremendous potential to disseminate information beyond the geographical boundaries. Diverse activities are possible over the internet which might not have even envisioned by its inventors. The process has not yet ended, it is still evolving. The commerce is one of the major areas which have been impacted by the internet. The traditional market structure has been changed. In fact, the whole world has been turned into a market place. Major advantages have been unfolded both for seller as well as the buyer. The seller now may reach any part of the globe and the buyer has unlimited choice to access any seller. Efficiency has been tremendously increased, paper work reduced, time lag shortened and expenses lessened. Among the many issues raised by Cyberspace are fundamental questions relating to the formation of contract and jurisdictional issues. All the facets of the business transaction with which we have

been accustomed in physical environment, can be now executed over the internet including, on-line advertising, on-line ordering, publishing, banking, investment, auction and professional services. Besides, many advantages offered by the information technology, a number of challenges have been also posed on the existing legal system.

3.1. Meaning and Concept of E-Contract

This is an undisputed fact that E-Commerce has become a part of our daily life. E-Commerce is the practice of buying and selling goods and services through online consumer services on the internet. The 'e' used before the word 'commerce' is a shortened form of 'electronic'. The effectiveness of E-Commerce is based on electronically made contracts known as E-Contracts. Although E-Contracts are legalized by IT Act, 2000 but still majority feels insecure while dealing online. The reason being lack of transparency in the terms and conditions attached to the contract and the jurisdiction in case of a dispute that may arise during the pendency of a transaction with an offshore site.[1]

In the words of *Sir William Anson*, a contract is a legally binding agreement between two or more persons by which rights are acquired by one or more to acts or forbearance on the part of the other or others. E-Contract is an aid to drafting and negotiating successful contracts for consumer and business E-Commerce and related services. It is designed to assist people in formulating and implementing commercial contracts policies within e-businesses. It contains model contracts for the sale of products and supply of digital products and services to both consumers and businesses.[2]

An E-Contract is a contract modelled, executed and enacted by a software system. Computer programs are used to automate business processes that govern E-Contracts. E-Contract can be mapped to inter-related programs, which have to specify carefully to satisfy the contract requirements. These programs do not have the capabilities to handle complex relationships between parties to an E-Contract. An

---

1 Rishabh Khandelwal, "Understanding E–Contracts and Its Impacts" *available at: http*://accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html(last visited on May 3, 2013).

2 Kapil Raina, "Evidentiary Value of E-Contracts," *available at: http://*www. legalserviceindia. com/article/l127-E-Contracts.html (last visited on February 5, 2013).

electronic or digital contract is an agreement drafted and signed in an electronic form. An electronic agreement can be drafted in the similar manner in which a normal hard copy agreement is drafted.[3]

For example, an agreement is drafted on your computer and was sent to a business associate via e-mail. The business associate, in turn, e-mails it back to you with an electronic signature indicating acceptance. An E-Contract can also be in the form of a "*Click to Agree*" contract, commonly used with downloaded software: The user clicks an "*I Agree*" button on a page containing the terms of the software license before the transaction can be completed. Since a traditional ink signature is not possible on an Electronic Contract, people use several different ways to indicate their electronic signatures, like typing the signer's name into the signature area, pasting in a scanned version of the signer's signature or clicking an "*I Accept*" button and many more.[4]

E-Contract is a contract modelled, specified, executed and deployed by a software system. E-Contracts are conceptually very similar to traditional (paper based) commercial contracts. Vendors present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payments. Then, the vendors deliver the purchased products.[5] In other words, it can be said that Electronic Contracts are contracts that are in a digital form. It can be defined as an agreement which is created in a digital form without using paper and pen. Online shop fronts, electronic market places, online auction sites, business to business and business to consumer infrastructures are different ways or form of a click to agree contracts,[6] commonly used with downloaded software.[7]

A contract is the primary mechanism for the transaction of business. A contract may be described as an agreement under which parties assume obligations to each other for valuable consideration. A contract may be governed by the law of the jurisdiction agreed between the parties or by the law of the jurisdiction imposed by

---

3 *Supra not.*1.

4 *Ibid.*

5 *Ibid.*

6 F. Tasneem, "The Legal Issues of Electronic Contracts in Australia" 1(2) *International Journal Management Business Research* pp.85-92 (2011).

7 Kapil Raina, "Evidentiary Value of E-Contracts" *available at: http://* www.legal serviceindia. com/article/l127-E-Contracts.html (last visited on February 5, 2013).

the court. Underlying the common law of contract is an assumption of freedom to contract with any person on any terms. While this assumption has been eroded over time through statutory reform and equitable doctrine, the basic premise still applies in relation to contract formation. The law prescribes the general elements of a binding contract but it does not require a contract to be formed by any particular method or to be in any particular form. It is accepted that a contract can be formed by a variety of methods including:

(i) An exchange of correspondence through the post, by telex or by facsimile;

(ii) Orally, either in person or by use of a telephone; or

(iii) By completion of a formal document.

A contract is not generally required to take a particular form and may be oral, provided there is no specific statutory requirement for the contract to be in writing. The advent of the internet as a means of facilitating contract formation does not, at first blush, present a situation different to that applicable to a facsimile or telex. An Electronic Contract may be formed either through an exchange of email or by completion of a document on an internet web-site which is submitted to another party electronically. There are three broad categories of subject matter for Electronic Contracts:[8]

(i) Sale of physical goods – goods are ordered over the internet with payment via the internet but delivery occurs in the usual way;

(ii) Sale of digitized products – goods such as software can be ordered, paid for and delivered on-line;

(iii) Supply of services – examples include electronic banking, sale of shares, financial advice, or consumer advice.

While it may be possible to view these methods as presenting a modern dimension to the accepted methods of contract formation rather than requiring any particular changes to the law, the electronic medium presents some particular issues arising from their electronic form.

---

[8] Sharon Christensen, "Formation of Contracts by Email – Is it Just the Same as the Post?" 1(1) *Queensland University of Technology Law and Justice Journal* p. 25 (2001).

It is required by the law that to prove a valid and binding contract at common law the following elements should be established:

(i) A valid offer has been made by one party to another;

(ii) The offer has been accepted by the other party or parties;

(iii) There is an intention by all parties to create legal relations when they entered into the contract;

(iv) The promises made within the contract are for valuable consideration and

(v) The terms of the contract are certain[9]

An Electronic Contract is an agreement created and 'signed' in electronic form. In other words, no paper or other hard copies are used. For example, you write a contract on your computer and e-mail it to a business associate, and the business associate e-mails it back with an electronic signature indicating acceptance. An E-Contract can also be in the form of a 'Click to Agree' contract, commonly used with downloaded software. The user clicks an 'I Agree' button on a page containing the terms of the software license before the transaction can be completed. The United Nations General Assembly Resolution No. A/ RES/51/ 162, dated 30th January 1997, Chapter III and specifically Article 11 sets about the formation and validity of E-Contract. Article 11 states that in the context of the contract formation unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data message. Where data message is used in the formation of a contract that contact shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.[10]

Simultaneously, Article 12 states that as between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of a data message. According to UNCITRAL Model Law, Article 11 is not intended to interfere with the law on formation of contracts rather to promote international trade by providing augmented legal certainty as to the conclusion of contracts by

---

9 *Ibid.*

10 S. J. Tubrazy,"E-contracts in Cyber Space," *available at: http://* www.articlesbase.com /cyber-law-articles/econtracts-in-cyber-space-502731.html(last visited on March 5, 2011).

electronic means. In certain countries a provision along with the lines of provision of Articles 11 might be regarded as merely stating the obvious, namely that an offer and an acceptance can be communicated by any means, including data message. Such reservations may stem from the fact that, in certain cases, the data message expressing offer and acceptance are generated by computer without instantaneous human intervention, thus raising doubts as to be expression of intent by the parties. Another reason of such uncertainties is inherent in the modes of communication and results from the absence of a paper document. As to the time and place of formation of contracts, in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation. It was felt that such a provision might exceed the aim of the Model Law which should be limited to providing that electronic communication would achieve the same degree of legal certainty as paper-based communication. The continuance of existing rules on the formation of contracts with the provisions contained in Article 15 is designed to drive out uncertainty as to the time and place of formation of contract in case where the offer or the acceptance are exchanged electronically.[11]

3.2. Essentials of E-Contract

An electronic or digital contract is an agreement drafted and signed in an electronic form. An electronic agreement can be drafted in the similar manner in which a normal hard copy agreement is drafted. The normal rule of contract law applies to the Electronic Contracts also.

Traditional concept of contract provides for the foundation of all types of valid and enforceable contract, keeping in view the meaning of definition of contract in Section 2(h) of The Indian Contract Act, 1872 as *an agreement enforceable by law and further requiring that it should be made by the free assent of parties, competent to contract, for a lawful consideration and with a lawful object and should not be expressly declared to be void.*[12] Hence it is clear that every contract needs certain conditions to be fulfilled which are known as essential ingredients of a contract. Contract exists only when following terms are fulfilled:

(l) An unconditional offer should be made

---

11 *Ibid.*

12 See, Sec. l0 of The Indian Contract Act, 1872.

(2) That offer should be accepted unconditionally

(3) There must be some consideration passing between the parties

(4) The parties are having intention to bind themselves and

(5) The agreement must be legally binding upon the parties

These are the necessary conditions without which no agreement will be a valid contract. It is to be noted that the rules of normal contracts are also applicable in the Electronic Contracts, hence Electronic Contracts also need few conditions to be fulfilled and the basic principle is same as in normal contract with slight modifications as discussed below:

3.2.1. Offer

An offer is a proposal made on certain terms by the offeror together with a promise to be bound if the offeree accepts the stipulated terms. An offer can be made expressly: an employer writes to a prospective employee to offer him a job impliedly, or by conduct: clicking a computer mouse.[13]The offer can be made to a specific person or to a group of persons or to the public at large. When the offer is made to a specific person or a group of person it can be called as bilateral and when it was made to public at large it is called unilateral offer.

In *Carlil* v. *The Carbolic Smoke Ball Company,*[14] the company advertised in a number of news papers saying that it would pay £100 to anyone who caught flu after using its smoke ball for 14 days. The company further stated that it had deposited £1,000 at a bank to meet possible claims. Mrs. Carlill bought one of the smoke balls, used it as directed and still caught flu. She claimed the reward but it was refused, so she sued the company in contract. The company put forward many arguments. One of such is that the offer was made with the whole world, which was clearly impossible. The court held that the company had made an offer with whole world and it would be liable to anyone who came forward and performed the required conditions.

An offer is to be distinguished from an invitation to treat. In invitation to treat, a person holds himself out as ready to receive offers, which he may then either accept

---

13 Sarabdeen Jawahitha, Noor Raihan Ab Hamid, "Electronic Contract and The Legal Environment", *available at: http://* www.irfd.org/events/wf2003/papers_global/R38.pdf (last visited on February 15, 2013).

14 (1893) 1 QB 525.

or reject. This is not an offer but merely it is a preliminary communication while in negotiation, the display of goods with price tag attached, advertisement, and auction can be considered as examples of invitation to treat.

In the case of *Eckhardt Marine GMBH* v. *Sheriff Mahkamah Tinggi Malaya & Ors*,[15] the Sheriff of the Seremban High Court advertised a motor vessel at Port Dickson for sale. The appellant wanted to buy the vessel and made an offer. The offer was sent to the Sheriff, under cover of the appellant's letter dated 12th February 1998, together with a banker's draft for 10% of the purchase price. The letter made it clear that the offer was on the Sheriff's terms but subject to two conditions. The Sheriff accepted the appellant's offer. The Court of Appeal held that the advertisement is an invitation to treat and the subsequent offer from the appellant created a binding contract. Regarding the invitation to treat the learned judge Gopal Sri Ram JCA stated that:

> *"An advertisement is considered by courts to be not an offer but a mere invitation to treat, that is to say, an offer to make offers."*

Consequently, under the Information Technology Act, 2000, the offer is made, unless otherwise agreed between the originator and the addressee, at the time when the electronic record enters any information system designated by the addressee for the purpose, or, if no system is designated for the purpose, when the electronic record enters the information system of the addressee, or, if an information system has been designated, but the electronic record is sent to some other information system, when the addressee retrieves such electronic record. This reflects the Model Law as to when an offer is made. The Act further provides that an electronic record shall be attributed to the originator if it was sent

(a) by originator, or

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record, or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

---

15 (2001) 3 CLJ 864.

This will presumably cover situations when an intelligent `agent' is programmed to issue offers on behalf of an individual. But does not cover where a file containing the offer is found by another.[16]

In this regard the European Union Directive on E-Commerce will be of great assistance. The Directive in Article 11 states that a consumer who is accepting a service provider's offer is a real offer and not an invitation to treat from the provider to make offers, and a real acceptance, and not an offer from the consumer. *Cavanillas* explains that the reason for this provision is to avoid giving the supplier or merchant a freehand to conclude the contract or not.

However, if the advertisers would like to treat the advertisements as invitation to treat, the invitation to treat and offer must be spelt out unequivocally. Before a customer is permitted to purport to make a purchase order, a statement should be made on a web site in a prominent place that the holding out of the goods or services on such web site constitutes an invitation to treat only and is not an offer. Further, safeguards may be installed by creating a 'checkout counter' icon on the web page and by making it mandatory for the customers to click on to the icon before the offer of the purchase procedure can be completed and also clearly stating that the client will conclude the contract.

3.2.1.1. Termination of An Offer

An offer can come to an end in a number of ways:[17]

1. Once the offer is accepted by the offeree;
2. By rejection. It can be rejected if:
    a. The offeree informs the offeror that he is not accepting the offer;
    b. The offeree wants to accept but subject to certain conditions; and
    c. The offeree makes a counter-offer.
3. By lapse of prescribed or reasonable time of acceptance.
4. Failure to fulfil conditions required on death or mental disorder of offerer.

---

16 Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

17 Sarabdeen Jawahitha, Noor Raihan Ab Hamid, "Electronic Contract and The Legal Environment", *available at: http://* www.irfd.org/events/wf2003/papers_global/ R38.pdf (last visited on February 15, 2013).

Revocation may be effective anytime before the offeree accepts the offer provided that the revocation is communicated to the offeree. If the acceptance is to be made by post like e-mail, the revocation must be communicated before posting.[18]

In *Byne* v. *Tienhoven,*[19] the defendant, on 1 October, posted letter of offer to the plaintiff and the plaintiff received the offer on 11 October and accepted by telegram. But the defendant posted a revocation letter dated 8 October which was received by the plaintiff on 20 October. The court held that a binding contract is formed between the parties because the revocation of the offer posted on 8 October was not effective until 20 October when it was received by the plaintiff (offeree). On the internet, the offeror can revoke an offer using e-mail, but whether it can be revoked by placing a notice on a web site is doubtful. Since the revocation notice needs to be actually received by the offeree, a web display will probably not suffice. The offeror's freedom in revoking an offer depends on how quickly the revocation is produced and the convenient means of producing evidence on the reception of the revocation.

2.2. Acceptance

Once a valid offer is made the next stage for formation of a valid agreement is an acceptance of the offer. The acceptance must be made while the offer is still open. Section 2(b) of the Contract Act states that when the person to whom the proposal is made signifies his assent thereto, the proposal is said to have been accepted. A proposal, when accepted, becomes a promise. The acceptance must be absolute and unqualified.[20] Meaning that the offeree agrees to each and every term in the offer and does not add additional terms. If the offeree adds additional terms in the acceptance or requests a change in the offer, the offeree has made a counter offer and becomes the offeror. In *Caspi* v. *Microsoft Network, L.L.C.,*[21] the U.S. court accepted the validity of an additional clause after conclusion of a contract.

Similarly, in *Rich and Enza Hill* v. *Gateway 2000 Inc.,*[22] the plaintiffs purchased a Gateway 2000 computer based on the telephone conversation. When the plaintiffs received the computer, the box contained additional terms including

---

18 *Ibid.*
19 (1880) 5 CPD 344.
20 See, Sec. 7 of The Indian Contract Act,1872.
21 323 N.J. Super. 118, 732 A.2d 528 (1999).
22 U.S. Court of Appeals for the Seventh Circuit 105 F. 3d 1147 (1997).

arbitration clause. The plaintiffs were given option to accept the additional terms within 30 days. When the computer did not function effectively the plaintiffs filed a suit in the court arguing that they should not be bound by the terms of the arbitration clause because they did not know about when they entered into the contract. The court of Appeal held that the terms are enforceable because the plaintiffs were given with an option of returning the items within a specified 30 days which they failed. By not returning the item, the buyer implicitly accepted the seller's conditions. Therefore, the plaintiffs should refer the case to the arbitration.[23]

Under The Indian Contract Act, 1872, the acceptance of a valid offer results in a valid contract. Such an acceptance may be expressed, in written or oral form or may be implied by the conduct of the offeree. The timing of an acceptance depends upon the context of mode of communication as inter praesentes means when the contracting parties are face to face with each other or inter absentees means where the contracting parties are not face to face with each other). Section 4 of Indian Contract Act, 1872 states acceptance is complete as against the offeror, when it is put in the course of transmission; the communication of acceptance is complete as against the offeree, when it reaches the knowledge of offeror.

In E-Commerce environment, there are four possible ways to convey acceptance:

- by sending an e-mail message of acceptance, or
- by delivery online of an electronic or digital product /service, or
- by delivery of the physical product, or by any other act or conduct indicating acceptance of the offer.

The IT Act, 2000 provides that the acceptance is binding on the offeree when the acceptance is out of his control, and binding on the offeror when he receives the acceptance. This differs from the position under the Contract Act. Section 12 of the IT Act, 2000 provides for a default acknowledgement process, if the originator and the addressee have not agreed upon the particular method of acknowledgement. It is provided that an acknowledgement may be given by Any communication by the addressee (automated or otherwise) or any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. Section 12(2) of the IT Act, 2000 stipulates further that "*where the originator has stipulated that the*

[23] *Supra note.* 13.

electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have never been sent by the originator."

> This provision prima facie appears reasonable, but it can lead to unrealistic situations. To illustrate, *if A sends a message and insists on an acknowledgement and B responds with an acknowledgement, but with a rider that acknowledgement must be acknowledged, then A and B may be constantly acknowledging each other's message and may never be able to complete the loop. If one of them does not acknowledge the receipt of the other's message, then the other's message will be deemed as never sent. This may result in the previous message being deemed as never sent, which would affect the earlier message and so on!*

Thus, such legal fiction can create issues that lead to ridiculous situations. It must be noted however, that the provisions of the ITAct, 2000 requires that they should be interpreted in tune with the provisions regarding the manner in which offers and acceptances are communicated and revoked under the contract act.[24]

3.2.3. Intention to Create Legal Relation

An agreement itself does not create a binding contract. It must be shown that the parties had the intention to be legally bound. Even if the Contract Act is silent, the case law (legal precedent) had shown the necessity of this element to form a valid contract.[25] The general presumption is that the business agreements are intended to face the legal consequences unless the parties specify otherwise. In the context of online contract, the existence of intent is normally automatic. However, an unclear or deceptive web site may dupe a consumer into making an unwanted contract. For example, an online merchant offering a digitized service may construct a web site which gives no purchasing information and merely displays the product and a 'Save' or 'Download Now' button. An unsuspecting customer will assume that the service is

---

24 *Supra note.* 16.

25 See, In *Phiong Khon* v. *Chonh Chai Fah* (1970) 2 MLJ 114, FC, A Chinese lady, who had a daughter and a son (respondent), lived together with the appellant after her first husband death. The respondent had executed a document which the appellant alleged was a transfer of land to him. The respondent denied. The Federal Court held that the appellant has to prove that the transfer was on his name which he failed. The Court further held the terms of the document create doubt that shows that there was no intention to create a legal relationship.

free and has no intention of creating a contract when the customer clicks the button. After the digitalized service has been delivered, the online merchant cannot demand payment because of the customer's absence of intention to create legal relation.

To avoid this, the law should ensure that commercial web sites explicitly state the prices and terms of their digitalized services. The customer should go through a sub-sequence of web pages detailing the terms and conditions of the transaction before making a purchase. The European Union Council Directive on E-Commerce[26] requires 3 steps to be taken by the e-shop owner as a contractual process before concluding the contract. They are offer, acceptance and acknowledgement of receipt. This will ensure that the acceptor knows that he is entering into a contract and there will be legal consequences when there is a breach. It further requires providing an opportunity to e-consumers or buyers to detect and correct mistakes and errors. In other words there is requirement to take measures like 'double clicks' in the E-Commerce web site to ensure complete consent.[27]

3.2.4. Consideration

The agreement by offer and acceptance and intention to create a legal relation does not make a contract. There is a need for consideration. Each party must promise to do or give something for the other side. The element of exchange is known as consideration. Section 25 of the Contract Act, 1872 says that a contract without consideration is void. Consideration is as an act or abstinence or promise by a promisee or by any other person at the desire of a promisor. The consideration is of three types. They are executory, executed and past consideration. In executory consideration the parties exchange promises to perform acts in the future. The promise to pay for the car and the promise to deliver the car are considered as valid considerations.

In *Wong Hon Leong David* v. *Noorazman bin Adnan,*[28] the respondent promised the appellant to help him in conversion and subdivision of the appellant land. The appellant promised to pay him. These mutual promises were held as valid

---

[26] 87/102/EEC, *available at: http://* www.columbia.edu~mr2651ecommerce31st Statutes Electronic Commerce Directive.pdf(last visited on October 16, 2012).

[27] *Supra note.* 16.

[28] (1995) 3 MLJ 283.

consideration. Executed consideration is where one party promises to do something in return for an act of the other party.

> Section 25 (b) of The Indian Contract Act, 1872 states that "*an agreement made without consideration is void unless it is a promise to compensate a person who has already voluntarily done something for the promisor.*"

In *Kepong Prospecting Ltd.* v. *Schmidt,*[29] Tan applied for permit for iron ore. Schmidt had assisted him in his application. The application was granted and Tan had promised to Schmidt to pay 1% of the selling price of the iron ore. Later Tan's business was incorporated as company and the company had undertaken to pay that 1% as agreed between Tan and Schmidt. The company later did not pay Schmidt and he sued the company for the money. The court held that the action of assisting the company and the subsequent promise by the company are valid considerations. It is to be noted that some countries do not recognize past consideration as valid consideration.

In an online web based contract, the position is likely to be straight-forward between contracting parties in buying goods or services over the internet and very often the consideration is executed in nature. The customer has to do some positive act like paying by credit card or e-cash and the retailer will promise to perform his part. Another possible situation on consideration in online contract will be on 'click-wrap' agreements. A web site which offers free of charge services requires a customer to agree to certain terms and conditions, which exclude the liability or prohibit commercial use, before allowing, the customer to download the digitized service. The concern is whether a click-wrap agreement of such nature has any consideration. Since free software or access to a web site represents a benefit there is a possibility to hold that there is a consideration.[30]

3.2.5. Capacity

It is assumed that everyone is capable of entering into a contract. However, minors, mental patients and drunks are in need of the law's protection because of their age or inability to appreciate their own actions. Therefore, they are not competent to

---

29 (1968) 1 MLJ 170.

30 *Supra note.* 13.

enter into a contract. As a general rule, all agreements are contract if they are made by free consent of the parties competent to contract. Every person is competent if he is major, of sound mind and not disqualified from contracting by any of the existing law.[31] The main concern in an online contract is the possibility of minors entering into commercial contracts. Before going into details of liabilities of minors and E-Commerce companies, there is a need to look at the definition of a minor.

Generally a contract entered by a minor is void. In the often cited Indian case of *Mohori Bibee* v. *Dhurmodas Ghose*,[32] the Judicial Committee of the Priviy Council held that all agreement entered into by the minors are void. This case had been followed in the *Government of Malaysia* v. *Gurcharan Singh*,[33] In this case learned judge *Chan Min Tat* held that an infant is totally incompetent and incapable of entering into a contract and thus there is no contract on which he can be sued. The decision implies that Section 65 of The Indian Contract Act, 1872 will not be applicable to contracts entered by minors. This Section gives right to parties in a voidable contract who have received any benefit hereunder must restore benefit.

Similarly, had a minor purchased goods online using his parent's credit card, the minor or his next friend will be able to recover any money paid, even though the contract is discovered to be void. As a precautionary measure, the vendor should obtain as much information on the person clicking the "Accept" button as possible for evidentiary purposes in case enforcement of the terms of the license is required. The vendor also should take opportunity to obtain specific information from the purchaser, such as his/her name, address, age, etc.

The possibility for an e-business to enforce a contract entered into by a minor is where the minor misrepresented or cheated the other party of his age. However in the case of *Mahomed Syedol Ariffin* v. *Yeoh Ooi Gark*,[34] the plaintiff's action to enforce a contract entered into by a minor failed because the plaintiff failed to prove that there was a misrepresentation. Thus, the court held that the contract is void. Has the misrepresentation been proven in this case the court might have ordered the defendant to restore the benefit received as in UK. In UK the courts developed an

---

31 See, Sec. 10 of The Indian Contract Act, 1872.
32 (1903) 30 Cal 539.
33 (1971) 1 MLJ 211.
34 (1916) 2 AC 575, PC (Penang).

equitable principle of restitution which requires the infant to return the benefits received which are still in his possession.[35]

3.3. Kinds of Electronic Contract

An Electronic Contract is also known as a 'click-wrap', 'click-through', 'web-wrap', 'browse-wrap' or 'point and click' contract. This is an agreement presented and consummated entirely in an on-line environment; most often on the internet. These contracts are typically contracts of adhesion i.e., one-sided (in favour of the presenting party), boiler plate agreements presented to customers on a 'take-it or leave it' basis. There is little if no room to negotiate the contract and, if the customer does not accede to the agreement, he or she will be denied access to the product or service. The term, 'wrap' is a misnomer and has nothing to do with the manner in which such agreements are physically presented. 'Click-wrap' or 'browse-wrap' agreements take their name from 'shrink-wrap' agreements; written paper contracts that were included in the plastic shrink-wrapped packaging containing, most often, computer software.[36]

A significant similarity between click-wrap and shrink-wrap contracts relates to their manner of acceptance as legally binding agreements. Users of software purchased in shrink-wrapped packages have been held to have agreed to the terms of a shrink-wrap contract by virtue of opening the package and installing the software. Similarly, in some instances, the courts have held that the web user can be bound by an Electronic Contract by the simple act of downloading software or purchasing products or services on-line. In both cases, the end user may not necessarily have read, much less understood, the contract. The term 'click-wrap' comes from the fact that in order to accept the terms of the contract on-line, the party must 'click' with a mouse on an on-screen icon or box.[37]

The four basic forms of Electronic Contract are as follows:[38]

1. The Click-wrap or Web-wrap Agreements
2. The Shrink Wrap Agreements

---

35 *Supra note.* 13.

36 Jeffery E. Wittmann ,Vancouver, BC. "Electronic Contracts", Negotiation and Drafting Major Business Agreements Conference Federated Press (October, 2007)., *available at: http://* www. wdwlaw.ca/ELECTRONIC_CONTRACTS_111007_ 280312.pdf (last visited on April 5, 2013).

37 *Ibid.*

38 *Ibid.*

3. The Electronic Data Interchange
4. The E-Mail Contract

3.3.1. The Click-Wrap or Web-Wrap Agreements

The Click-wrap agreements are those whereby a party after going through the terms and conditions provided in the website or program has to typically indicate his assent to the same, by way of clicking on an 'I Agree' icon or decline the same by clicking "I Disagree." These types of contracts are extensively used on the internet, whether it be granting of a permission to access a site or downloading of software or selling something by way of a website.[39] These are the most common form of agreement seen over the internet. Here, the consumer has to give his express assent by clicking upon the "I Agree" button or "I Disagree" button to deny assent to terms and conditions presented for the usage of a particular website or software products therein, for downloads or selling of products.[40]

The famous case of *Hotmail Corporation* v. *Van $ Money Pie Inc,*[41] where the Court of Northern District of California indirectly upheld the validity of such licenses where it said, "that the defendant is bound by the terms of the license as he clicked on the box containing "I Agree" thereby indicating his assent to be bound. The Click-wrap agreements, also known as 'browser-wrap' agreements, allow a buyer to manifest assent to the terms of a contract by clicking on an acceptance button that appears while the buyer obtains or installs the product. A buyer cannot start using the software until he or she has clicked on the button accepting the terms and conditions of the agreement. Click-wrap agreements require buyer action in order to begin usage but do not guarantee cognizance of the agreement terms. Buyers can assent to the contract without even reading it in order to use the product. Buyers cannot negotiate and must, therefore, accept the terms in entirty. Most courts find these agreements enforceable. Understandably, concern remains that click-wrap agreements may be

---

39 "Online Contract and Its Validity," *available at: http://* ashishlal.wordpress.com /2011/02/12/online-contract-in-context-of-internet/(last visited on November 15, 2012).

40 Siya Rathore, " Electronic Contracts: Understanding Digital Goods and their Sale and Purchase" *available at: http://* expertscolumn.com/content/electronic-contracts-understanding -digital-goods-their-sale-and-purchase (last visited on November 10, 2012).

41 C98-20064 (N.D. Ca, April 20, 1998).

accepted without users actually reading or understanding contract terms when manifesting assent.[42]

A clickwrap agreement is mostly found as part of the installation process of software packages. It is also called a click through agreement or clickwrap license. The name clickwrap comes from the use of shrink wrap contracts in boxed software purchases.

Click-wrap agreements can be of the following types:[43]

1. Type and Click where the user must type 'I accept' or other specified words in an on-screen box and then click a 'Submit' or similar button. This displays acceptance of the terms of the contract. A user cannot proceed to download or view the target information without following these steps.
2. Icon Clicking where the user must click on an 'OK' or 'I agree' button on a dialog box or pop-up window. A user indicates rejection by clicking "Cancel" or closing the window. Upon rejection, the user can no longer use or purchase the product or service. A click wrap contract is a 'take-it-or-leave-it' type of contract that lacks bargaining power.

The terms of service or license may not always appear on the same webpage or window, but they must always be accessible before acceptance.[44]

3.3.1.1. Types of Click-Wrap Contracts

In an off-line contract, both parties typically indicate their agreement to the terms and conditions thereof by signing. On-line, only one of the parties (usually, the surfer or person using the computer), signifies acceptance by 'signing' in the following ways:

1. Type and Click – the user must type 'I accept' or other words in a specified area and then click 'send'
2. Clicking an Icon – the user simply clicks an 'I accept' icon to go to the requested page; and

---

42 Rishabh Khandelwal, "Understanding E–Contracts and Its Impacts" *available at: http*://accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html (last visited on May 3, 2013).

43 Rohas Nagpal, "Ecommerce - Legal Issues" *available at: http://* www.asianlaws.orglibrary cyber -lawselectronic-contracts.pdf (last visited on July10, 2012).

44 *Ibid.*

3. Scroll and Click – the user must scroll down the terms of the click-wrap contract and then click an icon marked 'I accept' or 'I agree'.

One of the unique features of a click-wrap contract is that it is a one-sided, "take-it-or-leave-it" proposition. Unlike a paper contract, where the parties may vigorously negotiate the terms of the agreement before signing, the user in the on-line environment has no bargaining power. The user must either accept the terms of the click-wrap agreement (which will typically be in favour of the proffering party) or not gain access to the desired webpage, product or service. The lack of negotiation is partly due to the realities of on-line commerce, it is not logistically possible for the ISP or on-line service provider (OSP) to negotiate with each and every user.

3.3.1.2. Purposes of Click-Wrap Contracts

The main purposes of click-wrap agreements are to:[45]

1. Ensure contractual certainty.
2. Allow access to a particular web site or webpage.
3. Download software.
4. Purchase a product or service.
5. Inform the user of proprietary material on the web site.
6. Enumerate a web site's terms of use or service and privacy policy.
7. Impose limitations on the use of downloaded material.
8. Make it easier for the ISP or OSP to pursue users for violations or infringement.
9. Limit the ISP's or OSP's liability for use of content, errors or problems associated with downloaded software, other products or services.

3.3.2. Browse-Wrap Agreements

The Browse-wrap agreements, as distinct from 'click-wrap' agreements, do not require the active consent of the user. Acceptance of a browse-wrap is implied from the user's browsing or other activity on the web site, even if the user has not reviewed the Electronic Contract. Browse-wrap agreements are typically found at the

[45] *Ibid.*

bottom of a webpage in the form of a link to another page on which the terms and conditions are posted. The user is not required to review the contract, much less access the page where it is located, in order to proceed.

3.3.2.1. The Shrink Wrap Agreements

The Shrink-wrap agreements have derived their name from the "shrink-wrap" packaging that generally contains the Compact Disc Random Online Memory (hereinafter referred to as CD ROM) of Software. The terms and conditions of accessing the particular software are printed on the shrink-wrap cover of the Compact Disc (hereinafter referred to as CD) and the purchaser after going through the same tears the cover to access the CD ROM.[46] Sometimes additional terms are also imposed in such licenses which appear on the screen only when the CD is loaded to the computer .The user always has the option of returning the software if the new terms are not to his liking for a full refund.[47]

Shrink Wrap Agreements- CD-ROM of software is enclosed in shrink-wraps, which are the source for naming these agreements as Shrink-Wrap Agreements. The terms and conditions for using software are given on the shrink-wrap cover of the CD. The buyer first clearly reads the terms and conditions on the shrink-wrap cover and then tears it to access the CD-ROM. Few terms of license may appear after the CD has been loaded to the computer. The buyer has the option of returning back the software, if the new terms are not to his liking and can obtain a full refund of the price paid.

The case of *Step-Saver Data Sys., Inc.* v. *Wyse Tech,*[48] was the first time that a shrink-wrap agreement was contested. The Step-Saver had purchased a software program from the defendants by placing an order for 20 copies over the telephone, and had resold it to end-users. These customers brought a suit against the plaintiffs for the software's defects and they in turn sued the defendants in this case. Wyse Tech raised the disclaimer and limitation of remedies contained in the shrink-wrap license

---

46 "Electronic Contracts-A Basic Understanding," *available at: http://*www.lexvidhi.com/ article -details/electronic-contracts-a-basic-understanding-41.html(last visited on April 5, 2013).

47 "Online Contract and Its Validity" *available at: http://* ashishlal.wordpress.com /2011/02/12/ online- contract-in- context-of-internet/(last visited on November 15, 2012).

48 939 F.2d 91 (3d Cir. 1991).

as its defense. The Court of Appeals for the 3rd Circuit accepted the plaintiff's argument that the contract had been formed during the telephone conversation in which an offer to purchase had been made, and was accepted. The additional terms of the shrink-wrap license were construed as proposals for addition to the contract, and were not enforceable because Step-Saver had not assented to them. Hence, the liability for the defective software was placed on its manufacturer, rather than a reseller.

The validity of Shrink-Wrap Agreements came into consideration for the very first time through the leading case of *ProCD, Inc* v. *Zeidenburg,*[49] Pro CD had compiled data from 3000 telephone directories into a searchable database at a considerable expense. This data was sold on CD-ROM disks and the usage of the same was restricted by a License attached therein. The User's Manual contained the license and the license appeared every time the program was run by a user. Ziedenburg purchased this CD-ROM and uploaded the database on the internet, in contravention of the enclosed license in the CD-ROM. The Court held that the very fact that purchaser after reading the terms of the license featured outside the wrap license opens the cover coupled with the fact that he accepts the whole terms of the license that appears on the screen by a key stroke, constitutes acceptance of the terms by conduct.[50]

The Shrink-wrap agreements operate slightly differently. For example, they are used when one purchases off-the-shelf software. The agreement is imprinted on the software box, CD-ROM case, or other materials included inside the package. The license begins when the purchaser reads its terms and tears open the cellophane wrapping or shrink-wrap that surrounds the package. Buyers are supposed to return the software package to the retailer if they elect not to abide by the agreement. Courts are similarly concerned about buyers actually receiving notice of the sale, consciously agreeing to the sale, and conditioning the sale on acceptance of the license.[51] Shrink wrap contracts are license agreements or other terms and conditions which can only

---

49 86 F.3d 1447 (7th Cir. 1996).

50 Siya Rathore, " Electronic Contracts: Understanding Digital Goods and their Sale and Purchase",*available at:http://*expertscolumn.com/content/electronic-contractsunderstanding-digital-goods-their-sale-and-purchase (last visited on November 10, 2012).

51 Rishabh Khandelwal, "Understanding E–Contracts and Its Impacts" *available at: http://* accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html(last visited on May 3, 2013).

be read and accepted by the consumer after opening the product. The term describes the shrink wrap plastic wrapping used to coat software boxes, though these contracts are not limited to the software industry.[52]

The first case that discussed the concept of shrink-wrap licenses was the case of *Step-Saver Data Systems, Inc* v. *Wyse Technology,*[53] Step-Saver Data Systems, Inc was a company that configured and sold computer systems to various customers. These configured systems were purchased from a company known as The Software Link, Inc and the computer terminals were bought from Wyse Technology. Due to certain grave problems in the operating software, the customers of Step-Saver Data Systems, Inc brought suit against the latter. Since the suit against Step-Saver was based on the failure of the software to perform as promised, Step-Saver immediately filed a suit against The Software Link and Wyse Technology, alleging a breach of warranty. Step-Saver lost this case before the lower court. While the Court of Appeals for the Third Circuit affirmed the lower court's decision regarding the breach of contract provisions, it reversed (and this is interesting from the point of view of this discussion) the decision of the lower court with regard to the legal effect of the shrink-wrap license. The court held that since Step-Saver purchased the software program over the telephone, the contract for purchase of software was completed when the seller completed his obligations under the contract, by sending the software to the purchaser. Whatever terms were discussed over the telephone were the terms agreed to and since the seller did not mention any additional terms (such as those contained in the license agreement) that were incorporated in the contract, the court held that the purchaser was not bound by those terms. The purchaser learned about those additional terms only after payment and delivery of the software were complete. Thus, at the time the contract for purchase of software was completed, the purchaser had not expressly assented to the license agreement, since its terms were unknown to him.

Consequently, the contract that bound the purchaser to the terms of the license agreement was not accepted by the purchaser and therefore not enforceable by the seller. The court also held that it could not infer that the buyer had assented to the

---

52 Rohas Nagpal, "Ecommerce-Legal Issues" a*vailable at: http://* www.asianlaws. orglibrary cyber- lawselectronic-contracts.pdf (last visited on July10, 2012).

53 939F2d91 (3rdCirI991).

terms of the license from his conduct in continuing with the agreement. Since the buyer never expressly assented, the shrink-wrap license was not part of the contract for the sale of software and the terms of the license agreement could not be enforced.

The next significant case that alluded to the enforceability of shrink-wrap licenses is *Arizona Retail Systems, Inc* v. *Software Link, Inc*.[54] In this case, software Link sent a demonstration copy and a real copy of the software program to a prospective customer, Arizona Retail Systems, Inc. The complete terms of the shrink-wrap license agreement were printed on the outside of the envelope containing the real copy of the disk. The terms of the license agreement included some of the typical clauses contained in shrink-wrap licenses including clauses stating that:

- The customer has not purchased the software itself, but merely has obtained a personal, non-transferable license to use the program;
- The seller disclaims all warranties, except for a warranty covering physical defects in the medium on which the software is supplied;
- The purchaser's remedies were limited to repair and replacement of defective disks, and that the seller would bear no liability for damages caused by the use of the program;
- The license was the final and complete expression of the parties' agreements with regard to the software;
- The program or license could not be assigned without the express prior consent of the seller;
- The purchaser was deemed to have accepted the license upon opening the package containing the real copy of the software.

An analysis of these two cases indicates that, in the Step-Saver decision, the shrink-wrap license agreement was held to be unenforceable due to the fact that the terms of the purchaser's acceptance had not been communicated to the seller. All that had been communicated was an acceptance over the telephone that the purchaser was agreeable to purchase the software at the specified price. When the additional terms of the software license accompanied the software in terms of the shrinkwrap license agreement, the purchaser did not communicate his acceptance of the terms of the

[54] 831 F Supp 759 (D Ariz 1993).

license agreement to the seller and, the court refused to treat the continued use of the software by the purchaser as agreement on the part of the purchaser to the terms of the license agreement. This decision indicated the reluctance of the court to accept the newly created concepts relating to acceptance of contract terms that were created by the software industry. On the other hand, in the Arizona Retail case, the court appears to have agreed that the terms of the shrink-wrap license were in fact binding on the parties as a contract that has been duly accepted (acceptance being assumed from the licensee's silence) but since the terms of the license agreement were not reiterated on each copy of the software delivered, these terms were binding only in respect of the first copy.[55]

Thus, while the first case expresses serious reservations with regard to whether shrink-wrap license agreements constitute valid and binding contractual obligations, the second case seems to acknowledge the binding nature of contract created in such a manner but specifies that the contract must be repeated in respect of all copies of the software supplied, in order for it to be enforceable with regard to subsequent copies of the software.

3.3.2.1.1. Enforceability of Shrink-Wrap Contract

The question of enforceability of shrink-wrap licenses was raised once again in the landmark case of *ProCD* v. *Zeidenberg*.[56] The brief facts of this case are as follows:

ProCD, Inc was a company that had created a comprehensive national telephone listing database. This computer readable database contained details such as the full names, street addresses, telephone numbers, zip codes and industry codes for more than 95,000,000 residential and commercial properties. ProCD sold this database, bundled with another program, to three different groups of consumers at three different prices. The least expensive and limited use version was sold to members of the public, who intended to utilize the software for personal use only. For a higher price, a commercial version of the program was sold which did not have any limitations on the use of the data. In addition, ProCD also sold access to the program and the database, to users of the internet through America Online.

---

55 Rahul Malthan,*The Law Relating to Computers and The Internet* p.108 (Butterworths India, New Delhi, 1st edn.,2000).

56 86 F 3d 1447.

In order to make the proposed price discrimination meaningful, ProCD had to restrict the use of the program depending on the purpose for which the software had been purchased. Thus, if the software had been purchased for personal use alone, the purchaser had to be restrained from utilizing the software for any other purpose. While it was possible to restrict, by altering the software code, purchasers who had bought the product for personal use, from accessing all of the information on the database, there was no way in which the software could prevent such purchaser from utilizing the data which they were allowed to access from being used for commercial purposes. In order to restrict the use of the data, all non-commercial versions of the program were supplied under a shrink-wrap license that obligated the purchaser to utilize the software only for personal use.

The terms of the license agreement were included in the user guide contained in the package. It stated as follows: Please read this License carefully before using the software or accessing the listings contained on the discs. By using the discs and the listings licensed to you, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, promptly return all copies of the software, listings that may have been exported, the discs and the User Guide to the place where you obtained it.

The license went on to inform the user that the ProCD software was copyrighted and that copying the software was authorized only for the particular purposes and uses that were specified. The program was such that once the product was installed on the user's computer, the program reminded the users that the product and the data was subject to the Single User License Agreement and that the products were licensed for authorized use only. Once again, before the user was allowed to access any of the listings, a message appeared on the computer screen, stating listings contained within this product are subject to a License Agreement. Please refer to the help menu or to the user guide. The shrink-wrap license itself did not mention the terms of the contract in full. There was, however a reference to the agreement, in small print, at one place on the box.

In order to determine the validity of the shrink-wrap license, the court first examined whether Zeidenberg had assented to the terms of the license agreement. In this case, the box was encased in the shrink-wrapping and at the bottom of the box was a message in small print. Though this message stated that the purchaser was

subject to the terms and conditions of the enclosed license until the purchaser removed the shrink-wrapping, he would not be able to read the terms of the license found inside the box.

Relying on the decision in the earlier cases of *Step-Saver Data Systems, Inc* v. *Wyse Technology*[57] and *Arizona Retail Systems, Inc* v. *Software Link, Inc,*[58] the court came to the conclusion that unless the terms of the license agreement are apparent to the purchaser at the time the contract is concluded, the purchaser would not be bound by the contract. A mere reference to the existence of a contract is not enough. The purchaser needs an opportunity to read all the conditions before conveying his acceptance and since the 'potential incorporation of the terms can occur only after the purchaser opens the package and has a reasonable opportunity to inspect the user agreement', the buyer was not in this case, given the opportunity to expressly assent to the terms of the shrink-wrap license. Consequently these terms could not be enforced. This was held, by the lower court, to apply not only to the first purchase of the software, but to subsequent purchases of upgrades as well.

In the recent decision of *Mortenson Company* v. *Timberline Software corporation,*[59] the court held that the terms of the license agreement that was shipped along with the software to the purchaser, (including provisions of such license agreement relating to the limitation of the consequential damages recoverable) was a part of the contract between the parties. There was little argument that the terms of the license agreement were clearly visible to the parties, as the full text of the license agreement appeared on the outside of the sealed cover containing the software as well as on the inside cover of the user manual shipped with the product and on the introductory screen of the program, each time the program was executed. The license also stated that the use, by the purchaser, of the program, amounted to an agreement on the part of the purchaser to be bound by the terms of the license. If the user did not wish to be bound by those terms, such user was permitted to return the program to Timberline for a full refund of the purchase price.

The court came to this conclusion even though the purchaser agreed to buy the software after a negotiation in respect of the price of the software during which

---

57 939 F 2d 91 (3rd Cir 1991).
58 831 F supp 759 (D Ariz 1993).
59 1999 Wash App Lexis 185 (Wash Crt App, 1 Feburary 1999).

negotiation, the terms of the license were not mentioned, and even though the purchaser confirmed its agreement to purchase the software under a purchase order that was sent to a dealer of the seller, prior to the receipt by the purchaser of the terms of the license. The court, in this decision seems to have completely veered away from the ruling in the *Step-Saver* and whole heartedly adopted the decision in *ProCD* v. *Zeidenberg.*

An analysis of this decision indicates, that the court agreed to uphold the contract on the basis that:

- The purchaser had, at the time when he gave his assent to the contract, notice that additional terms exist;
- The purchaser had the opportunity to review the terms of the license; and
- The purchaser was allowed the opportunity to reject the terms, return the software, and obtain a refund if he thought the terms were objectionable.

It may also be appropriate to examine the concept of click wrap licenses, which is fast becoming an important method for concluding contracts on the internet. Briefly explained, a click wrap contract is one by which purchasers of software or services, who utilize the internet to make such purchases, become bound, by means of a contract to abide by certain restrictions or obligations. This contract is, in many respects, similar to the shrink-wrap contract in that it contains similar terms as to applicable contractual restrictions and manner of use. The difference lies in the fact that unlike shrink-wrap licenses that are concluded when the customer tears the shrink-wrapping and proceeds to use the software, click wrap licenses are concluded when the purchaser of these services clicks on a button on the screen (that normally says 'I Agree') signifying their assent to the terms of the contract. The essentials of contract formation are adhered to in that the purchaser of services has the opportunity to read the contract and then click on the button signifying his/her agreement with the terms of the contract. More importantly, such purchaser cannot proceed to explore other areas of the website unless he/she has clicked on the button to signify that he/she agrees with the terms of the contract.

Recently, the United States District Court for the Northern District of

California in the case of *Hotmail Corporation* v. *Van Money Pie Inc*,[60] upheld the validity of click wrap contracts using the same reasoning as was used in as ProCD to uphold shrink-wrap licenses. Hotmail is a pioneer in the free e-mail service business and has a customer base of over 10 million customers. In order to utilize hotmail services, the client is required to register and during the process of registration, must agree to the terms of service published by hotmail on its website. One of the prohibitions set out under the terms of service, is that users are prohibited from using hotmail e-mail accounts to facilitate the transmission of unsolicited commercial e-mail, (more colloquially referred to as spam). Users are given an opportunity to view all the terms of service and to signify their acceptance of these terms of service by clicking on a box that indicates the user's acceptance.

The leading case on browse-wrap agreements is *Specht* v. *Netscape Communications Corp,*[61] where free downloads of Netscape's software obtained web-usage information from its users, presenting privacy concerns. The browse-wrap terms included an arbitration clause. Upon installation, users were merely told to please review and agree to the terms of the Netscape Smart Download software license agreement before downloading and using the software. The court ruled that this was an invitation and not a condition, and could not constitute assent. Providers of online services and software have the option of click-wrap agreements, and have to bear with the consequences of failing to use it. However, it appears that terms on a browse-wrap agreement would bind competing businesses.

Based on the foregoing cases, businesses would do well to keep some best practices in mind while deploying E-Contracts:

(1) Online agreements should be as conspicuous as possible.
(2) Whenever possible, use click-wrap rather than browse-wrap and the viewing of the terms should be mandatory. This could be accomplished by graying out accept until the user has scrolled to the bottom on the agreement.
(3) A notice should be included near the, 'Accept' button to make the user grasp the significance of his actions, such as "By clicking Accept, you are entering into a legally binding agreement."
(4) Keep a record of the moment that the user clicked 'Accept'.

---

60 C98-20064 (ND Ca, 20 April 1998).
61 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

In order to come to such a conclusion, the court had to first hold that both parties were bound by an enforceable agreement. Since the preliminary injunction was granted, the court appears to have indicated its willingness to uphold the validity of a click wrap agreement, and held *Van Money Inc* to be bound by the plaintiffs terms of service solely by clicking 'I agree' after being presented with an opportunity to view the terms of service.

3.3.3. E-Mail Contact

The general rule is that an acceptance must be communicated to the offeror. The contract is formed at the place and time the acceptance is received by the offeror. If the post is used for acceptance the acceptance is effective immediately upon regardless the letter is delayed or lost provided it is properly stamped, addressed and posted. The postal rule is applicable to telegram too, but not to more instantaneous means of communication such as telex, telephone. As for the instantaneous means, the general principle will be applicable. The acceptance is effective only when it comes to the knowledge of the offeror.[62]

Anyone interested in communicating business details through e-mail must have an e-mail address for which he has to register himself with an internet service provider who runs a constantly accessible mail server. Once the registration is complete, an electronic mail box (inbox) along with the address is allocated to the user. The person wishing to send an offer to another will type the desired contents of the offer on his system with an e-mail address of the party to whom he intends to send the offer which is to be mentioned in the address column. The message is then electronically transmitted by pressing the 'send' button to the service provider of the sender and is then forwarded to the recipient's provider who puts it in the recipient's mail box where it is saved. Placing e-mail in the recipient's mail box does not enable him to know the contents of the message. This will be possible only when he queries his mail box from his own system by inserting ID (user name) and password. Similarly, the sender does not know whether the recipient has received the message.[63]

---

62 Sarabdeen Jawahitha, Noor Raihan Ab Hamid, "Electronic Contract and The Legal Environment", *available at: http://* www.irfd.org/events/wf2003/papers_global/R38.pdf (last visited on February 15, 2013).

63 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* p.137 (2001).

It is the view of some commentators that e-mail should be treated as another form of instantaneous communication requiring acceptance to be communicated to be effective. It is the writer's view that to consider a classification of e-mail as either instantaneous or non-instantaneous means may lead to the application of the postal acceptance rule in inappropriate situations. A more appropriate approach is to start with the general rule followed by a consideration of whether the general rule is displaced by reference to the intentions of the parties, by sound business practice or a consideration of where the risks should lie. Consequently, no one formulation may be applicable to all situations due to the large number of permutations and, in any event, any formulation may need to be revised in light of changes to technology.[64]

Similarly, with the advent of information technology, the issue of communication of acceptance needs to be revisited as regards to e-mails and web based acceptance. An e-mail communication is first sent to the Internet Service Providers (hereinafter referred to as ISP). The ISP will then send that message to the actual recipient, when the recipient sends a request to his ISP to download the messages that it has received and are addressed to the recipient only. Once the downloading is completed, the message actually will reach the recipient. Looking at the manner in which an e-mail communication operates one may say that e-mail is akin to postal rule. The offeror is bound by the acceptance once the acceptance is put in a course of transmission to the proposer so as to be out of the power of the acceptor. Thus, once the message is sent by the acceptor to his ISP, the message can be considered out of the control of the offeree.

If the general principle is applied, an acceptance sent by e-mail will be effective at the time it is communicated. Communication in the type of system described above could occur at the time the message is received by the recipient's ISP or at the time the message is downloaded to the recipient's computer or at the time the message is read by the recipient. Does this mean that because no definite time of communication can be readily identified that a different rule, such as the postal acceptance rule, should be applied? The postal acceptance rule has not been applied to other forms of modern communication such as facsimiles and telexes.

---

64 Sharon Christensen,"Formation of Contracts by Email – Is it Just the Same as the Post?" 1(1) *Queensland University of Technology Law and Justice Journal* p.32(2001).

Some commentators suggest that e-mail should be treated in the same way as telexes. While this has some appeal from a commercial perspective it cannot be justified by reference to the equality of the technology. Telexes were viewed as not being strictly instantaneous, but there was a consensus that they should be treated as if it were an instantaneous communication between principles, like a telephone conversation. A parallel may be drawn between the use of a telex and the use of Electronic Data Interchange (hereinafter referred to as EDI). As EDI creates a direct link between the parties it may be viewed as a virtually instantaneous form of communication. An EDI system could be compared to the sending of a facsimile direct from one facsimile machine to another. In this particular instance it is submitted that the general rule should apply and acceptance should be effective at the time it is received by the other party. However, an email sent over the internet does not travel directly from one computer to another but rather through a number of third party computers.[65]

3.3.4. The Electronic Data Interchange (EDI)

Electronic Data Interchange means the electronic transfer from computer to computer of information using an agreed standard to structure the information.[66] It is also defined as the electronic interchange of machine processable structured data which has been formatted according to agreed standards and which can be transmitted directly between different computer systems with the aid of telecommunication interface with or without human intervention. Before the advent of the internet, business communities used to execute their contracts by electronic data interchange.[67] It facilitates direct electronic exchange of business information between computers in a computer processable format and is generally used by the parties having continuing business relationship. These parties, before establishing any contractual relationship, generally exchange an agreement called a 'trading partner agreement' in which the details about the warranties, disclaimers, liabilities and the relevant rules which will be applicable in case of dispute, are mentioned. In pursuance to trading partner

---

65 *Ibid.*

66 See, Article 2(b) of UNCITRAL Model Law on Electronic Commerce, *available at http://*www.uncitral.org/english/text/electron/ml.ec.htm. (last visited on April 15, 2013).

67 See, Graham J H Smith, *Internet Law and Regulation* p.207(Sweet and Maxwell, London, 2nd edn.,1999).

agreement parties transmit through EDI, purchase orders, acceptances and invoices.[68]

Similarly, EDI is the computer-to-computer transmission of information used by frequently contracting commercial parties to send and receive standard forms, generally purchase orders and invoices, in a store and forward message system. It is, perhaps, the clearest example of electronic contracting through the use of an electronic agent. Parties agree on the standardized terms of the transaction. Transactions, quotes and automatic responses to them, are sent and received daily via a phone line between electronic agents, devoid of human involvement. EDI reduces the time and complexity associated with sending and receiving large volumes of information, reducing keystroke errors. Purchase orders are one of the most common uses of EDI. For example: Wal-Mart, a large retailer, uses EDI to repeatedly order large quantities of consumer goods, such as laundry detergent, for its thousands of stores. EDI enables the ordering and invoicing of these goods between computer systems. Contract, offer, acceptance, and assent occur automatically.[69]

3.4. Evidentiary Value of Electronic Contract

3.4.1. Evidence: Meaning and Concept

Evidence in its broadest sense includes anything that is used to determine or demonstrate the truth of certain assertion. Giving or procuring evidence is the process of using those things that are either (a) presumed to be true or (b) were themselves proven via evidence. Evidence is a currency by which one fulfils the burden of proof. In simple words anything that makes the things in question evident to the court is evidence. Similarly, any law in the area should be indicative of positive acceptance of the use of information technology and dynamism to facilitate its growth. The proliferation of Computers/Internet has created a number of problems for the law. Many legal rules assume the existence of paper records, of signed records, of original record.[70]

The Law of Evidence traditionally relies on paper records as well though of course oral testimony and other kinds of physical objects have always been part of

---

68 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* pp. 133-170 (2001).

69 Rishabh Khandelwal, "Understanding E–Contracts and Its Impacts" *available at: http*:// accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html(last visited on May 3, 2013).

70 V.D.Dudeja, *Cyber Crimes and Law* p. 95(Commonwealth Publishers, 1st edn., 2002).

court-rooms, too. As more and more activities are carried out be electronic means, it becomes more and more important that evidence of these activities by available to demonstrate the legal rights that flow from them. The term reliability has caused confusion between the principles of authentication, best evidence, hearsay and weight. There has been a growing demand from industry and users for new types of signatures to effectively substitute the hand written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents. The advent of the internet is similar to that of the telephone, telegraph, and fax machine communication is facilitated.[71]

The key to admissibility of E-Commerce transactions and documents is the evidence of data integrity. A pre-condition to the admissibility of a record in the judicial proceedings is its authentication, which can be satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Digital agreements, invoices and related e-mails and other digital communications must be authenticated with respect to its origin and accuracy of storage, retrieval and printing or other visual display. Due to the common perception that electronic file are susceptible to purposeful or accidental alteration or incorrect processing, authentication of digital evidence may require, in some situations a higher level of foundational proof thant traditional evidence.[72]

Consequently, Section 14 of the IT Act 2000 provides *"an electronic record would be deemed 'secure', if 'any security procedure' has been applied to an electronic record.*" It shall be deemed secure from the time the security procedure was applied up to the point in time of verification. It is not clear what could amount to a 'security procedure' valid under this Section, though the scope seems to be very wide. A secure electronic record and a secure digital signature can avail of beneficial provisions in the amended Evidence Act. The IT Act, 2000 states that a file produced by techniques that accurately reproduce the original will be admissible as the original itself. This admissibility is curtailed if a bona fide question is raised as to the authenticity of the

---

71 *Ibid.*

72 Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

original. Further output readable by sight, or a printout of data is stored on a computer will be construed as original.[73]

3.4.2. Concept of The Electronic Evidence

The evidentiary value of an electronic record totally depends upon its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records. According to Section 3 of The Indian Evidence Act, 1872, "*evidence means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence*". For the purpose of Section 79A of The IT Act, 2000 Electronic Form evidence means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, cell phones, and digital fax machines. Thus the section clarifies that documentary evidence can be in the form of electronic record and stands at par with conventional form of documents. The proliferations of computers have created a number of problems for the law. The advent of the internet is similar to that of the telephone, telegraph and fax machine. Thus communication is facilitated thereby. The internet must be facilitated. The legal environment aims at facilitating the use of technologies to best serve society. The focus on drawing the balance between conflicting goals of safeguarding and facilitating electronic transactions that encourages transparency and uniformity in the legal system. Almost all evidence to prove facts is litigation involving the Internet-Computer generated because technology today allows for internet usage through computers.[74]

However, technology is fast embracing mobile technology where users can access the internet, use e-mail and receive faxes etc. by mobile phones through the Wireless Application Protocol (WAP). Internet service through television and cable companies-these modes of communication involves processing the transaction through a mechanical device. The Indian Evidence Act, 1872 does not define a computer but allows for copies to be made by mechanical processes. Reference to computer and media are made as regards Evidence in the Companies Act, 1956. It is necessary to harmonize the principles in the various Laws such as the Evidence Act and the Companies Act after the enactment of The IT Act, 2000 and the changes in the legal system. Computer generated documentary evidence consists of a

---

73 V.D. Dueja, *Cyber Crimes and Law* p.95(Commonwealth Publishers, 1st edn., 2002).

74 *Id.* at p.96.

Calculations or analysis that are generated by the computer through the running of software and the receipt of information from other devices. Real evidence arises in many circumstances. If a bank computer calculated the bank charges due from a customer based upon its tariff, the transaction on that account and the daily cleared credit balance etc., this calculation would be a piece of real evidence .[75]

Evidence recorded or stored by availing the electronic devices is given the evidentiary status. For instance: the voice recorded with the help of a tape recorder, the digital voice recorder, digital cameras, digital video cameras, video conferencing have been added to new evidentiary assets. Justice *Gururajan*, of the Karnataka High Court in *twentieth century fox film* v.*NRI Film Production Associates,* [76] has already held in a civil suit that video conferencing evidence is valid evidence. The emergence of information and communication witnessed sea change by elevating the status of the evidence recorded, generated or stored electronically from the secondary to primary evidential status. The shift in the paradigm owes to the efforts of the working group of the United Nations Commission on International Trade Law (UNCITRAL) Model law on Electronic Commerce and assigning of the legal recognition to e-record or data message.[77] The position of e-documents in the form of SMS, MMS and email in India is well demonstrated under the law and the interpretation provided in various cases.

In *State of Delhi* v. *Mohd Afzal & Others,*[78] it was held that electronic records are admissible as evidence. If someone challenges the accuracy of a computer evidence or electronic record on the grounds of misuse of system or operating failure or interpolation, then the person challenging it must prove the same beyond reasonable doubt. The court observed that mere theoretical and general apprehensions cannot make clear evidence defective and inadmissible. This case has well demonstrated the admissibility of electronic evidence in various forms in Indian courts. In this case, *K.K. Velusamy* v. *N. Palanisamy,*[79]Supreme court observed in this case that the amended definition of "evidence" in Section 3 of the Evidence Act, 1872 read with the definition of "electronic record" in Section 2(t) of the Information Technology Act 2000, includes a compact disc containing an electronic record of a conversation. Section 8 of Evidence

---

75 *Ibid.*

76 AIR 2003Kant 148.

77 Kapil Raina, "Evidentiary Value of E-Contracts" *available at: http://*www. legal serviceindia.com/article/l127-E-Contracts.html (last visited on February 5, 2013).

78 2003(3) 11 JCC 1669.

79 MANU/SC/0267/2011.

Act provides that the conduct of any party, or of any agent to any party, to any suit, in reference to such suit, or in reference to any fact in issue therein or relevant thereto, is relevant, if such conduct influences or is influenced by any fact in issue or relevant fact, and whether it was previous or subsequent thereto.

3.4.3. Admissibility of Electronic Evidence

All the legislatures in the world are in favour of the electronic evidence. They say that these evidences cannot be denied admissibility only on the ground that they are electronically made or stored. The legal response in this regard may be summarized as under:

3.4.3.1. The United Nations Commission on International Trade Law (UNICTRAL) Modal Law

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) deals with the admissibility and evidentiary weight of data message in Article 9(1). The article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message solely because it is a data message (electronic format). It clearly states that data messages should not be denied admissibility on the sole ground that they are in electronic form. It also suggests that due evidential weight must be given to information presented in the form of a data message. The criteria for assessing the evidential weight shall include the following:[80]

I. The reliability of the manner in which the data message was generated, stored or communicated.
II. The manner in which the integrity of the information was maintained.
II. The manner in which its originator was identified, as well as any other relevant factor that might arise.[81]

3.4.3.2. Uniform Electronic Transactions Acts (UETA)

The Act makes it clear that contracts and signatures are not unenforceable merely because they are in electronic form. But the law has never required that most contracts be written down, let alone written down on paper rather than stored

---

[80] Mathew Biji Thomas, "Evolving Legal Framework Governing Electronic Commerce"4 *Indian Journal of International Law* p. 35(2001).

[81] *Ibid.*

electronically. And for those contracts that were required to be signed and in writing (notably, contracts for the sale of goods and real estate contracts), the courts were come to the conclusion that an electronic writing and an electronic signature would satisfy the requirement. Still, the Act will give businesses more peace of mind concerning the enforceability of their electronic transactions. More and more contracts and other transactions will likely be conducted electronically, particularly as the technology involved in ensuring the security and authenticity of electronic signatures and in determining possession of notes and other negotiable documents in electronic form improves.[82] The provision of the Act says about the electronic record under Section 7 as a record created, generated, sent, communicated, received or stored by electronic means. The major substantive provision of the Act are as.[83]

(1) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(2) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

3.4.4. Information Technology Act, 2000 and Electronic Evidence

The Information Technology Act, 2000 lays down a blanket permission for records not to be denied legal effect if they are in electronic format, as long as they are accessible for future reference. Section 4 of The IT Act, 2000 provides for legal recognition of electronic records. It says that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference.

The Indian Evidence Act, 1872 excludes the word ‘written’ from the definition of ‘document’ and says that a 'document' means any matter expressed or described upon any substance by means of letters, figures, or, marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of

---

82 Nandan kamath, *Law Relating to Copyright Trademarks and Patent* p.96 (Universal Law Publishing Co. Pvt Ltd,2nd edn.,2006).

83 *Ibid.*

recording that matter. The focus of this statute (Indian Evidence Act, 1872) is on the purpose of the document which is to be used for recording the matter and no matter whether it is written or not. The Act further provides that documents must be proved by primary evidence to satisfy the best evidence rule. But there are exceptions to this rule also. The only way to examine electronic documents for recording is by displaying it on a secondary device, either a screen or a printout. It is tenable argument that such a display is not original, but amounts to a copy, and is, therefore, as a general rule inadmissible in evidence. This issue requires further attention to eliminate any doubt.[84]

3.4.4. Evidentiary Value under Indian Evidence Act, 1872

The evidentiary value of electronic records in India can be understood with reference to Sections 85A, 85B, 85E, 88A and 90A of the Indian evidence Act, 1872. These provisions deal with the presumptions as to electronic agreements, electronic records, electronic signature certificates and electronic messages. Section 65 B relates to the admissibility of electronic records. The above mentioned sections are worth noting with brief explanation.

Section 85A of the Indian Evidence Act, 1872 [85] **:** This section is incorporated as regards presumption to electronic agreements. It says that

> *"every electronic record of the nature of an agreement is concluded as soon as the electronic signature is affixed to the record."*

Section 85A has been added in order to ensure the validity of E-Contracts. But there are some restrictions as regards the presumptive value. The presumption is only valid to electronic records, electronic records that are five years old and electronic messages that fall within the ambit of Section 85B, Section 88A and Section 90A of Indian Evidence Act.

> **Section 85B of the Indian Evidence Act, 1872**: Section 85B provides that *"the court shall presume the fact that the record in question has not been put to any kind of alteration, in case contrary has not been proved."*

---

84 Nandan kamath, *Law Relating to Copyright Trademarks and Patent* p.96 (Universal Law Publishing Co. Pvt Ltd,2nd edn.,2006).

85 Ins.by Information Technology Act, 2000(Act No.21 of 2000),Section 92 and Schedule 2.

The secure status of the record may be demanded till a specific time. The digital signature should also be presumed to have been affixed with an intention of signing and approving the electronic record. Further it has been provided that the section should not be misread so as to create any presumption relating to the integrity or authenticity of the electronic record or digital signature in question. Section 85E:

> *"As far as electronic signature certificate is concerned, the court shall presume that the information listed in the certificate is true and correct."*

Inclusion of the words 'shall presume' again relates to the express exclusion of the discretionary power of the court.

> **Section 88A of the Indian Evidence Act, 1872**[86]: *"The court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission. But the court shall not make any presumption as to the person by whom such message was sent."*

This section is self-explanatory as it purports to follow the basic rules of a valid hard-copy agreement. The words may presume authorize the court to use its discretionary power as regards presumption. Sections 85A and 85B contained the words 'shall presume' which expressly excluded this discretionary power of the court.

Section 90A of the Indian Evidence Act, 1872[87]: In case of an electronic record being 5 years old, if proved to be in proper custody, the court may presume that the electronic signature was affixed so as to authenticate the validity of that agreement. The electronic signature can also be affixed by any person authorized to do so. For the purpose of this section, electronic records are said to be in proper custody if they are in the custody of the person with whom they naturally be.

Section 65B of the Indian Evidence Act, 1872: Section 65B talks about admissibility of electronic records. It says that

> *any information contained in an electronic record which is printed on a*

---

86 Adv Prashant Mali, "E-contract: Now Admissible in Court" *available at: http://* dqindia.ciol.com/content/ top_stories/2010 /1010122701.asp (last visited on March 5, 2013).

87 *Ibid.*

paper or stored/recorded/copied on optical/magnetic media produced by a computer shall be deemed to be a document and is admissible as evidence in any proceeding without further proof of the original, in case the following four conditions are satisfied:

- *The computer output containing such information should have been produced by the computer during the period when the computer was used regularly to store or process information for the purpose of any activities regularly carried on during that period by the person having lawful control over the use of the computer.*
- *During Such period information of the kind contained in the electronic record was regularly fed into the computer in the ordinary course of such activities.*
- *Throughout the material part of such period, the computer must have been operating properly. In case the computer was not properly operating during such period, it must be shown that this did not affect the electronic record or the accuracy of the contents.*
- *The information contained in the electronic record should be such as reproduces or is derived from such information fed into the computer in the ordinary course of such activities.*

It is further provided that where in any proceedings,

evidence of an electronic record is to be given, a certificate containing the particulars prescribed by Section 65B of the Act, and signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities would be sufficient.

Supreme Court in *State* v. *Navjot Sandhu,*[88] while examining the provisions of newly added Section 65B, held that in a given case, it may be that the certificate containing the details in sub-section 4 of Section 65B is not filed, but that does not mean that secondary evidence cannot be given. It was held by the court that the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, sections 63 and 65 of the Indian Evidence Act 1872. Paragraph 150 of the judgment which is apposite, reads as "Section 63, secondary evidence

[88] (2005) 11 SCC 600.

means and includes, among other things, copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies".[89]

Section 65 of the Indian Evidence Act, 1872 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal knowledge. Irrespective of the compliance with the requirements of section 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Indian Evidence Act 1872, namely, sections 63 and 65.[90]

In this case, *State of Punjab* v. *Amritsar Beverages Ltd. and Ors.,*[91]Supreme Court observed in this case as internet and other information technologies brought with them the issues which were not foreseen by law as for example, problems in determining statutory liabilities. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or did not have the sufficient insight to tackle with the new situation. Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus. Information Technology Act, 2000 although was amended to include various kinds of cyber crimes and the punishments therefore, does not deal with all problems which are faced by the officers enforcing the said Act. The Indian Penal Code, 1860 has been amended to include electronics documents within the definition of 'documents.' Section 63 of the Evidence Act has been amended to include admissibility of computer outputs in the media, paper, optical or magnetic form. Section 73A prescribes procedures for verification of digital signatures. Sections 85A and 85B of the Evidence Act raise a presumption as regards electronic contracts, electronic records, digital signature certificates and electronic messages.

---

89 *Supra note.* 88.
90 *Ibid.*
91 AIR 2006 SC 2820.

3.4.5. Relevant Amendments

With the introduction of the Information Technology Act, 2000 certain amendments are to be carried out in the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. These amendments will try and make these existing codes internet compatible. Section 29A has been specifically inserted in the Indian Penal code to provide that statutory balance. The said section introduces the term 'electronic records' in the code. This includes audio, video, data, text or multimedia file generated, stored, received or sent in any electronic form or microfilm or computer generated micro files[92]. Further the changes been brought up under Sections 167, 172, 173,175, 192, 204, 463, 464, 466, 468, 469, 470, 471,474,476,477A. The evidentiary value of an electronic record totally depends upon its quality. The Indian Evidence Act, 1872 has widely dealt with the evidentiary value of the electronic records. According to Section 3 of the Evidence Act, evidence means and includes all documents including electronic records produced for the inspection of the court and such documents are called documentary evidence. Thus, the section clarifies that documentary evidence can be in the form of electronic record and stands at par with conventional form of documents. As per the Information Technology (Amendment) Act, 2008, section 79A empowers the central government to appoint any department, body or agency as examiner of electronic evidence for providing expert opinion on electronic form of evidence before any court or authority.

3.5. Electronic Contract: Consumer Protection Issues

Important functions of the internet are to provide Information and knowledge, a mode of communication, which are effective, efficient and cost-friendly and a market for goods and services. Once the internet market becomes fully operational, civilization would witness a conversion of ordinary consumers to Cyber Consumers. Many products and services are available to cyber consumers through the internet whether it is online booking of air tickets or the purchase of consumer goods. The world market would be at the command of the cyber consumer through the screen of his/her P.C. This cyber consumerism would be the subject of legal protection available to consumers. The issues which arise in the cyber market deserve as much

---

92 Vakul Sharma, *Information Technology: Law and Practice* pp. 213-218 (Universal Law Publishing Co., 2nd edn.,2009).

importance as other issues of cyber crime, jurisdiction over the cyber world and taxation. Since, the cyber consumer does not come face to face with the seller in an online purchase of goods or hiring of services, the risk of defective goods delivered deficiency in services and other frauds may increase. As goods are purchased online from the Cyber market and delivered later, the cyber consumer does not get the opportunity to examine them. Retail web-shops can also disappear after booking orders and receiving payments through credit cards. The Law of consumer protection is significant in this age of e-consumerism. Every cyber consumer must understand the law or consumer protection. Similarly, E-Commerce players include manufacturers, suppliers, retailers and service providers in India and abroad need to be aware of the legal responsibilities towards them under the Consumer Protection Act, 1986.[93]

3.5.1. Cyber Consumer

The Information Technology Act, 2000 is silent on Cyber Consumerism and leaves this entire area to the Consumer Protection Act, 1986. The Consumer Protection Act, 1986 (hereinafter referred to as CPA) is a protective legislation against manufacturing defect in goods, deficiency in services, unfair trade practices and restrictive trade practices committed by manufacturers, traders and service provides. The CPA is the first codified legislation to protect the interest of consumers. Before the inception of the CPA, a consumer has to file a suit in the civil court to claim damages and compensation from manufacturers and traders for defects in their goods and from service providers. Though the CPA was legislated to ensure expeditious consumer justice, it does not serve the intended purpose due to lack of proper infrastructure for consumer courts and inadequate number of Judges in proportion to long list of consumer litigants. The CPA intends to relieve the consumers from arbitration proceedings or civil action. The peculiar facts and the circumstances, of a particular case come, to the conclusion that the appropriate forum for adjudication of the dispute would be given to the CPA such as by arbitration or remedy before the civil court the parties may be relegated to arbitration or civil court as the case may be where the consumer court finds that the case before it involves acute and serious questions of

[93] V.D. Dueja, *Crimes in Cyber Space: Scams and Frauds* p.183 (Commonwealth ,1st edn.,2003).

facts requiring examination of witnesses etc. It may relegate the parties to the remedy of filing a suit in the civil court.[94]

3.5.2. Definition of Consumer

The Consumer in Section 2(d) of the Consumer Protection Act, 1986 which is as follows Consumer means

> "*any person who buys any goods for a consideration which has been paid or promised or partly paid and partly promised or under any system of deferred payment and includes any user of such goods for consideration paid a promised or partly paid or partly promised or under any system of deferred payment when such use is made with the approval of such person but does not include a person who obtain such goods for resale or for any commercial use or hires or avails of any services for a consideration which has been paid and partly promised or under any system of deferred payment and includes any beneficiary of such services other than the person who hires or avails of the services for consideration paid or promised or partly paid and partly promised or under any system of deferred payment, when such services are availed with the approval of the first mentioned person*".[95]

However, a person who hires services for consideration shall be consumer whether or not the same are hired for any commercial purpose. In the case of services, the law does not provide for any exclusion as in the case of goods. For example, where a company engages the services of an architect to design its factory building, the said company shall be a consumer within the ambit of the definition irrespective of the fact that the services are hired for a commercial purpose. Therefore, in so far as services are concerned, all persons who hire services for a consideration are consumers, irrespective of whether they are manufacturers and traders requiring the services for a commercial purpose.

3.5.3. Good and Services

3.5.3.1. Goods

Goods means every kind of movable property other than actionable claims and money; and includes stock and shares, growing crops, grass, and thing attached to or

---

94 *Id.* at p.184.
95 *Ibid.*

forming part of the land, which are agreed to be severed before sale or under the contract of sale.

3.5.3.2. Service

Service has been widely defined to mean service of any description which is made available to potential users and includes the provision of facilities in connection with banking, financing, insurance, transport, processing, supply of electrical or other energy, boarding or lodging or both, housing, construction, entertainment, amusement or the purveying of news or other information, but does not include the rendering of any service free of charge or under a contract of personal service. Since the definition of service is inclusive, the various services provided therein are not exhaustive of the list and are only illustrative in nature meaning thereby that all services of any nature are covered under the definition, except free services or under a contract of personal service. Government companies, bodies and local authorities rendering services or selling goods are also covered under the CPA. All services rendered through the internet are also covered within the ambit of this definition. However, it is reiterated that free services, which are countless on the internet, are not covered under the CPA as per the exclusion in the definition of service. Duties, which are judicial, quasi-judicial and statutory in character, which are exclusive sovereign functions of the state, are not services under CPA. The officers implementing the registration act and stamp act do not render any service under the CPA, as they perform statutory duties to raise and collect state revenue, which is a part of a sovereign power of the state.[96]

3.5.4. Consumer Complaint

The Consumer Protection Act, 1986 can be invoked only if the complainant consumer makes any or more of the following allegations:

- The goods bought or agreed to be bought suffer from one or more defects.
- The services hired or availed of or agreed to be hired or availed of, suffer from deficiency in any respect.
- An unfair trade practice or a restrictive trade practice has been adopted by any trader, i.e. who sells or distributes goods for sale and includes the manufacturer.

---

[96] *Ibid.*

- A trader has charged for the goods mentioned in the complaint a price in excess of the price fixed by or under any law for the time being in force or displayed such a price on the goods or any package containing such goods. This clause includes cases where price above the MRP (Maximum Retail Price) is sought to be charged.
- Goods which are hazardous to life and safety when used, are being offered for sale to the public in contravention of the provisions of any law for the time being in force which requires traders to display information in regard to the contents, manner and effect of use of such goods.

3.5.5. Defect in Goods and Deficiency in Services

Defect means any fault, imperfection or shortcoming in the quality, quantity, potency, purity or standard which is required to be main tamed by or under any law for the time being in force or under any contract, express or implied or as is claimed by the trader in any manner whatsoever in relation to any goods. Cause of action for defect in the product, deficiency in service, unfair trade practice or restrictive trade practice, cannot in all cases be avoided by the manufacture, trader or service provider as the case may be, merely on placing reliance on a document containing the statement of the consumer to the effect that he is completely satisfied by the product or service. The mere execution of the discharge voucher would not always deprive the consumer from preferring his claim with respect to the deficiency in service. Despite execution of the discharge voucher, the consumer may be in a position to satisfy the consumer forums under the Act that such a discharge voucher or receipt had been obtained from him under circumstances which can be termed as fraudulent or exercise of under influence or by misrepresentation or the like. If in a given case, the consumer satisfies the authority under the Act that the discharge voucher was obtained by fraud misrepresentation, under influence; coercive bargaining compelled by circumstance or the like, the authority before which the complaint is made would be justified in granting appropriate relief.[97]

[97] *Id.* at p.186.

3.5.6. Reliefs under Consumer Protection Act, 1986

The Consumer forum as have the power to grant the following reliefs to aggrieved consumers against the opposite party.[98]

- To remove the defects from the goods in question.
- To replace the goods with new goods of similar description this shall be free from any defects.
- To return to the complainant the price paid by him and to pay such amount as may be awarded as compensation to the consumer for Any loss or injury suffered by the consumer due to the negligence of the opposite party.
- To remove the defects of deficiencies in the services in question.
- To discontinue the unfair trade practice or the restrictive trade practice or not to repeat them.
- Not to offer hazardous goods for sale.
- To withdraw the hazardous goods from being offered for sale and to provide adequate costs to the parties.

If the consumer forum is satisfied that the goods complained against suffer from any of the defects specified in the complaint or that any of the allegations contained in the complaint are proved, it has the power to order the opposite party to inter-alia pay compensation to the consumer for any loss or injury suffered by the consumer due to the negligence of the opposite party. Therefore, the following ingredients need to be proved by any aggrieved consumer before successfully claiming compensation against the opposite party: [99]

- The allegations in the complaint of the aggrieved consumer have been proved against the opposite party.
- The opposite party has been negligent.
- A loss of injury has been suffered by the aggrieved consumer as a consequence of the negligence of the opposite party.

---

98 *Ibid.*

99 *Id*.at p.184.

Consumers are often careless and mechanical while filing complaints against opposite parties in the consumer courts. Consumers negligently fail to plead negligence on the part of the opposite parties in their complaints. Many of the consumers only plead defect in the goods or deficiency in the services or unfair trade practices or restrictive trade practices adopted by a trader without pleading negligence. Deficiency in the services or defect in goods or unfair trade practices do not per se tantamount to negligence on the part of the opposite party except in a few cases where the act itself speaks of negligence and hence does not need to be proved separately. Negligence is the omission to do something, which a reasonable man, guided by those ordinary considerations, which ordinarily regulate human affairs, would do, or the doing of something, which a reasonable and prudent man would not do. Negligence is the failure to use such care as a reasonably prudent and careful person would use under similar circumstance or failure to do what a person of ordinary prudence would have done under similar circumstances. Negligence is the conduct, which falls below the standard established for the protection of others against unreasonable risk of harm. It is a departure from the conduct expected of a reasonably prudent person under like circumstances.[100]

3.5.7. Compensation under Consumer Protection Act, 1986

The Compensation under Consumer Protection Act, 1986 (hereinafter referred to as CPA) is only for any loss or injury suffered by the consumer because of the negligence of the opposite party. Loss means some detriment or deprivation or damage or injury. Compensation under CPA can be granted only when it is found that the person from whom damages are claimed is found to have acted negligently and such negligence must result in some loss to the person claiming damages. In other words, loss or injury if any, must flow from negligence. [101]

In a case where due to a strike by the employees, the bank could not function thereby causing hardships to the customers, the Supreme Court held that firstly there was no deficiency in the services since the shortcomings were not due to failure in the performance of the bank's duties or discharging it's obligations under the law and moreover even otherwise no loss or damage was caused to any depositor due to the negligence of the bank and hence no claim for damages under CPA was

---

100 *Id*.at p.188.
101 *Id*.at p.189..

maintainable. Compensation means indemnification or in other words that which is necessary to restore an injured party to its former position. It is the equivalent in money for the loss sustained. It is a settled principle of law that mental agony, if any, caused due to the negligence of the defendant can also be compensated in money. The quantification of compensation towards mental agony suffered by a consumer is a difficult question and very often, it ultimately boils down to the subjective discretion of the judicial foras.[102]

Usually the consumer foras in India have been extremely conservating in granting compensation towards mental agony suffered by consumers. It is only in those cases where death has occurred on a account of medical negligence or otherwise that consumer foras in India are a little more liberal but still are nowhere near their counterparts in the United Stated of America or the European countries. Every claim for compensation must be supported by evidence and material in support thereof without which no compensation can be granted. Bad claims have no remedy under the law.[103]

Where a person fails or omits to comply with any order passed by the District Forum, the State Commission or the National Commission, section 27 of CPA provides that such person shall be liable to be punished with imprisonment for a term which shall not be less than one month but which may extend to three years, or with fine which shall not be less than rupees two thousand but which may extend to rupees ten thousand, or with both. This provision provides teeth to consumer foras effectively enforce their orders. It is the fear of pension that consumer forum orders are in most cases religiously implemented in by the traders, manufacturers and service-providers against whom orders are passed.

3.5.8. Consumer Foras, Jurisdiction and Implications on Cyber Consumers in India

In the age of cyber consumerism, where products and services from all over the globe would be freely and easily available to Indian consumers, issues of jurisdiction of consumer foras are of significance. Issues of jurisdiction affect a consumer more than they affect any other person. It would be next to impossible for a domestic consumer of a product or service to seek redressal of his grievances if he has

---

102 V.D. Dueja, *Crimes in Cyber Space: Scams and Frauds* p.189 (Commonwealth ,1st edn.,2003).

103 *Ibid.*

to litigate in a foreign land. For Instance, if a consumer 'C' buys a Sony Television set from a retail website based in Japan, which is found to be defective, it would not be viable if C has no litigate in Japan. The multitude of consumers cannot even of litigating in foreign lands; hence, the subject of jurisdiction of consumer foras in India assumes relevance for them. [104]

A three tier redressed mechanism for aggrieved consumers are provided under the Consumer Protection Act. The three consumer disputes Redressal agencies established for the purposes of the Act are District Consumer Disputes Redressal Forum for every state and National Consumer Disputes Redressal Commission. Subject to the jurisdiction based upon pecuniary limits as state above, a consumer complaint is to be filed in the District Forum or State Commission as the case may be, having jurisdiction over either of the following places:[105]

- Where the opposite party or each of the opposite parties, where there are more than one, at the time of the institution of the complaint, actually and voluntarily resides or carries on business or has a branch office or personally works for gain.
- Where any of the opposite parties, where there are mere than one, at the time of the institution of the complaint, actually and voluntarily resides or carries on business or has a branch office, or personally works for gain, provided that in such case either the permission of the District Forum is given, or the opposite parties who do not reside, or carry on business or have a branch office or personally work for gain, as the case may be, acquiesce in such institution.
- Where the cause or action, wholly or in part, arises.

Territorial jurisdiction under consumer law is the same a under the civil law as provided in the Code of Civil Procedure, 1908 'Jurisdiction over the Cyber World'. Cause of action means the fact or facts, which give a person a right to judicial relief. It is a situation or state of facts, which would entitle a party to sustain action and give him the right to seek a judicial remedy in his behalf. Cause of action means the whole

---

104 *Ibid.*
105 *Ibid.*

material facts, which are necessary for the plaintiff to prove in order to entitle him to succeed in the suit. Cause of action includes the circumstances forming the infringement of the right or the occasion for the action. Cause of action in a consumer dispute ordinarily would arise in either or more of the following places, depending upon the nature of the dispute raised by the consumer.

3.5.8.1. Applicability of Consumer Protection Act, 1986 Foreign Goods is Sold or Services Provided to A Consumer in India

Foreign manufacturers and distributors may or may not be liable under the CPA for a manufacturing defect or deficiency of service or unfair trade practice or restrictive trade practice, depending upon different fact situations. In a case where a foreign manufacturer or distributor does not intend nor has any knowledge nor does it authorize the sale of its products in India, it would not be liable under CPA merely because its products are sold in India. The onus of proving such intention would however lie upon the foreign manufacturer.

In *Smith V. Hobby Lobby Stores Inc.* v. *8oto Co. Ltd.*,[106] Smith brought a wrongful death action against Hobby Lobby Stores Inc. Hobby Lobby Stores field a third-party complaint against Boto Co. Ltd. who was the maintaining as internet site, which was also accessible to residents of Arkansas. The court held that Arkansas did not have jurisdiction because Boto had no agent or distribution system in Arkansas. Moreover, Boto had not made any sale to Arkansas customers for five years prior to the action and Boto had no knowledge regarding the method or manner or transportation or distribution of its products by its customers. Therefore, the court held that there were insufficient contacts for jurisdiction in Arkansas. However, where the foreign manufacturer or distributor is conscious and intends that its products are sold in India, then such a manufacturer or distributor as the case may be, would be liable to the consumer under CPA for any manufacturing defect, etc. All retailers and service-providers based outside India, operating through the internet services if they sell goods or provide services to consumers in India. Thus, foreign retailers, service providers and the aforesaid category of conscious manufacturers and distributors, would be amendable to the jurisdiction of consumer foras in India because the cause of action in an ordinary sale of goods or hiring of services would substantially or at

[106] 1997 U.S. Dist. LEXIS 9828.

least partially arise in India. Cause of action in India in such cases would consist of any or more of the following facts taking place in India:[107]

- The consumer buys the goods or hires services from India.
- The goods are sold or services are provided to the consumer in India.
- The product is delivered or services are availed of in India.
- The consumer suffers the manufacturing defect or deficiency in services in India.
- The consumer makes payment for the goods from India.

Therefore, web sites intending to play in the market in India would have to exercise caution and adjust their actions in line with the law of consumer protection in India. This is not an impossible task for it requires proper legal planning in accordance with the laws in India. They must act like the Multi Nation Companies who do business globally by following the laws of the respective countries where they operate in.

3.6. Formation of The Electronic Contract And Information Technology Act, 2000

The time and place of a communication are relevant to the issue whether a contract has been concluded or not. The time of the contract indicates the time from which the parties are bound to act in accordance with the contract. This is also relevant in cases where actions are time-critical. The place of contract, on the other hand, plays an important role in establishing the jurisdiction for any cause of action due to breach. Further, the time and place may be also relevant to determine whether an obligation or a condition has been performed. Under the Contract Act, the modes to determination the time of the formation of a contract through various alternative forms of communication have examined in several cases. As regards postal contracts, a variety of theories has been propounded as follows.

(a) The theory that the contract is complete as soon as the offeree has made a declaration of his acceptance,

(b) The theory that the contract is formed when a letter or telegram has been dispatched accepting the offer, and

---

[107] V.D. Dueja, *Crimes in Cyber Space: Scams and Frauds* p.191 (Commonwealth ,1st edn.,2003).

(c) The theory that communication of the acceptance must be received by the offeror.

When the proposal and acceptance are made by letters, the contract is made at the time when and at the place where the letter of acceptance is posted.[108]

The Contract Act does not specifically deal with where a contract is concluded but courts in India have generally been guided by the common law principles where no statutory provision to the contrary is in existence. In *Entores Ltd.* v. *Miles Far Eastern Corporation*[109], it was held that in the case of oral communication or communication by telex or over the telephone, acceptance is communicated when it is actually received by the offeror and therefore the contract is deemed to be placed where it is received. *Denning, L.J.* observed:

> *When a contract is made by post ... acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. But there is no clear rule about contracts made by telephone or by telex... My conclusion is that the contract is only complete when the acceptance is received by the offeror: and the contract is made at the place where the acceptance is received. This view was accepted by the Supreme Court of India.*

The question now remains whether in the case of Electronic Contracts; a contract is concluded when the acceptance is dispatched from the sender or when the acceptance is actually received by the offeror. The Information and Technology Act, 2000 provides that the dispatch of an electronic record occur when it enters an information system outside the control of the person who sent the record, unless otherwise agreed. The time for receipt of an electronic record is determined by the time when the electronic record enters the computer resource designated by the addressee or if the electronic record is sent to a computer resource not designated by the addressee, it occurs at the time when the addressee retrieves the electronic record. Alternatively, if no computer resource has been designated, then receipt occurs when

---

[108] Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

[109] (1955)2 QB 326.

the electronic record enters the computer resource of the addressee. The Information and Technology Act, 2000 Act also sets default rules for the place of dispatch and receipt of documents. The electronic records are deemed to have been dispatched at the place the originator of the message has his principal place of business and received at the place where the addressee has his principal place of business. These rules as regards place of business are in consonance with the rules in this regard under the UNCITRAL Model Law, and are identical to those under the Singapore legislation.

3.6.1. Formation of a Contract and Application of Mirror Image Rule / the Mailbox Rule

The Common law principle that a contract comes into existence only when acceptance is a mirror image of offeror's offer has been given statutory recognition in the Contract Act. The rule is that a proposal will ripen into a promise only when acceptance is absolute and unqualified. Thus an acceptance with variation is not an acceptance but a counter proposal which must be accepted by the original promiser before a contract is made. An important qualification to this rule is that where an acceptance of a proposal is not absolute, the proposer may still be bound, if, by his subsequent conduct, it is shown that he has accepted additional conditions incorporated by the acceptor in his acceptance.[110]

When a counter proposal is accepted, a contract comes into existence and the terms of the contract are the terms of the counter proposal. This is called last shot doctrine which means that were conflicting communications are exchanged, each is a counter offer, so that if a contract results at all, it must be on the terms of the final document in the series leading to the conclusion of the contract.[111]

A contract is formed when acceptance is communicated to the offeree. This presents few problems in face-to-face negotiations, but when communicating over distances, it is often the case that the offeree has dispatched an acceptance which is not received by the offeror or arrives after the expiry of the offer.[112] Does acceptance

---

110 See, *Bhagwandas v. Shri Dial*, 1913 Punj Rec. No.92 p. 325.

111 See, *Simbia Steel and Building Supplies v. James Clerk and Eaton Ltd.* (1986) 2 Lloyd's Rep 225.

112 Sairam Bhat (eds.), *Law of Business Contracts in India* 199 (SAGE Publications India Pvt Ltd, 1st edn.,2009).

take effect when it was sent or when it arrives? Under sec. 4 of the Indian Contract Act, the communication of acceptance is complete:

1. As against the Proposer, when it is put in the course of transmission to him, so as to be out of power of the Acceptor, and
2. As against the Acceptor when it comes to the knowledge of the Proposer.

This mirrors early common law cases on the mailbox rule, wherein acceptance is deemed to be communicated to the offeree when it enters the postal system. Case law also tends to distinguish between delayed forms of communication and instantaneous forms of communication, such as the telephone, telex, and fax machine. Acceptances communicated using such mediums are formed when the offeror receives the acceptance because they are functionally equivalent to face-to-face communications. In *Entores Ltd. v. Miles Far Eastern Corporation,*[113] the plaintiffs made an offer to the defendant corporation in Holland. This was accepted by a telex, which was received on the plaintiff's machine in London.

> *Denning, L.J.* observed: "*When a contract is made by post ... acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. But there is no clear rule about contracts made by telephone or by telex... My conclusion is that the contract is only complete when the acceptance is received by the offeror: and the contract is made at the place where the acceptance is received."*

Similarly, in *B.G. Kedia v. G. Parshottamdas and Co.,*[114] the Supreme Court ruled that contracts concluded over the telephone, being an instantaneous mode of communication, would not be subject to the mailbox rule. Is it possible to extend the analogy to emails and other forms of computer mediated communication? Acceptances would be formed when the offeror receives the acceptance, and the transmitting party bears the risk of broken communications. The problem in adopting this is that most email systems use mail servers operated by third parties, and the recipient has to login to the mail server before he has a chance to read the communication.

---

113 (1955)2 QB 326.
114 1966 AIR SC 543.

Due to the unrestricted nature of Electronic Contracts, there is a possibility that an acceptance may not be mirror image of the offer. This "battle of forms'[115] is however, unlikely to arise in case of web based contracts. Generally a web page carries predetermined standard terms and conditions and the customer will have little scope to vary, modify or add any condition of his choice. E-mail, on the other hand, allows parties to append their own terms and conditions. The customer may e-mail a purchase order with its standard terms of purchase and supplier may use the same method of communication, accepting the order but appending its own terms and conditions of sale.[116]

The courts have found it sometimes difficult to determine whether a communication is a counter offer or not. It may not be sometimes clear from the communication of the offeree whether he is making a counter offer or merely seeking further information. This uncertainty is increased by the principle of 'last shot' as it is sometimes difficult to determine precisely the point of time when a contract comes into existence in a transaction which involves a series of negotiations. [117]

The Uniform Commercial Code of America has provided a solution to this problem by modifying the mirror image rule which echoes the essence of Article 19(2) of the Vienna Convention on Contracts for the International Sale of Goods. The Convention provides that a purported acceptance containing additional or different terms that do not materially alter the terms of the offer, constitutes an acceptance, unless the offeror, without undue delay, objects orally to the discrepancy or despatches a notice to that effect. If he does not so object, the terms of the contract are the terms of the offer with the modifications contained in the acceptance. The material alteration includes among other things, the price, payment, quality and quantity of goods, place and time of delivery, extent of one party's liability to the other or the settlement of disputes.[118]

It has been suggested in the Guide to Enactment of the UNCITRAL Model Law that the courts or other national authorities while enacting provisions of Model

---

115 'Battle of forms' is a term used where parties exchange incompatible set of standard terms.

116 Farooq Ahmad, *Cyber Law in India* p.219 (New Era Law Publication, 4th edn., 2013).

117 Farooq Ahmad, "Electronic Commerce: An Indian Perspective" 143(2) *International Journal of Law and Information Technology* p.62(2001).

118 Farooq Ahmad, *op.cit.*p.220.

Law or the provisions of the Instruments implementing the Model Law as a part of domestic legislation which, of course will be domestic in character, be interpreted with reference to its international origin in order to ensure uniformity. [119]

True to the spirit of the mirror image rule developed by the Common Law courts, Indian courts have followed it while determining the nature of the response of the offeree to an offer. Transactions over the internet are national as well as international in character. In order to bring Indian law at par with the international rules relating to the formation of the contract, for ensuring uniformity and at the same time to avoid uncertainty, modification of the above rule is needed.[120]

3.6.2. Law Relating to Written Documents

A contract may be required to be in writing or to be evidenced in writing. The General Clauses Act, 1897, in Section 3 (65) states that expressions referring to 'writing' shall be construed as including references to printing, lithography, photography and other modes of representing or reproducing words in a visible form. It is doubtful whether an Electronic Contract would have the requisite degree of visibility required for the General Clauses Act. under section 4 of Information and Technology Act, 2000 states that where a law requires information to be written or to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule if the information contained therein is accessible so as to be usable for subsequent reference. The Article 5 of the Model law states that where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.[121]

Soft copies may be accommodated under the definition of document as stated in Section 3(18) of the General Clauses Act 1897 states that document shall include any matter written, expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means which is intended to be used, or

---

119 Farooq Ahmad, "Electronic Commerce: An Indian Perspective" *144*(2) *International Journal of Law and Information Technology* p.62(2001).

120 Farooq Ahmad, *op.cit.*p.220.

121 Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

which may be used for the purpose of recording that matter. Information in soft copies is stored as bits and bytes; it may be argued that bits and bytes are stored in the electronic medium as zeros and ones. It can be contended that zeros and ones are figures or marks that are expressed on the disc, so that they fall within the definition of document. If the requirement of writing were satisfied, the definition of document for the purposes of the General Clauses Act, 1897 section Sec 3 (18) would also be satisfied since documents include any written matter. [122]

3.6. 3. Law Relating to The Evidence

Rights and remedies have no implication unless they can be enforced. Enforcement requires that a party prove, in accordance with the rules of evidence that a contract existed, what were its terms were, how it was breached and to what extent such party was damaged. As such the contractual documents must be admissible to the court that is it must comply with the evidentiary standards. The key to admissibility of E-Commerce transactions and documents is the evidence of data integrity. A pre-condition to the admissibility of a record in the judicial proceedings is its authentication, which can be satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Digital agreements, invoices and related e-mails and other digital communications must be authenticated with respect to its origin and accuracy of storage, retrieval and printing or other visual display. Due to the common perception that electronic file are susceptible to purposeful or accidental alteration or incorrect processing, authentication of digital evidence may require, in some situations a higher level of foundational proof that traditional evidence.[123]

Section 14 of the Information and Technology Act 2000 provides that an electronic record would be deemed 'secure', if 'any security procedure' has been applied to an electronic record. It shall be deemed secure from the time the security procedure was applied up to the point in time of verification. It is not clear what could amount to a 'security procedure' valid under this Section, though the scope seems to be very wide. A secure electronic record and a secure digital signature can avail of beneficial provisions in the amended Evidence Act. The Information Technology Act, 2000 states that a file produced by techniques that accurately reproduce the original

---

122 *Ibid.*
123 *Ibid.*

will be admissible as the original itself. This admissibility is curtailed if a bona fide question is raised as to the authenticity of the original. Further, output readable by sight, or a printout of data is stored on a computer will be construed as original.

The Model law states that where the law requires information to be presented or retained in original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented. The criteria for assessing integrity include the use of digital signatures. Further information in the form of a data message shall be given due evidential weight, after considering the reliability of the manner in which the data message was generated, stored or communicated, reliability of the manner in which the integrity of the information was maintained, the manner in which the originator was identified, and any other relevant factor.[124]

3.6.4. Contractual Agreement and Information Technology Act, 2000

The basis of a contract is an agreement. An agreement notionally comprises of an offer, which is then accepted. Offers may be made directly or through a mass e-mail or through a web page. It is important to distinguish an offer from an invitation to make an offer. Whilst a direct contact is likely to be construed as an offer, a mass email or advertisement on a web page may be either an offer or an invitation to make an offer. The distinction is important as an offer if accepted results in a contract whereas an invitation to offer required the recipient to make an offer, which may then either be accepted or rejected. A contract is concluded when an offer is accepted. If any advertisement over the web or any communication over the internet (automatic or otherwise) is construed as an offer, and if that offer is unconditionally accepted, the contract is concluded. On the other hand, if the advertisement is construed as an invitation to make an offer it only invites users to make an offer for the advertised

[124] *Ibid.*

product or service. The choice whether to accept that offer is in the hands of the person who invited the offer.[125]

An invitation to offer opens the process of negotiation. In order to identify such invitations the law has developed presumptions as to whether certain common statements or actions amount to an offer or are mere invitations to make an offer. Thus it can be said with some authority that shop displays are invitations to treat, as are items for sale at auctions and advertisements. A web advertisement is closer to shop displays than to advertisements in magazines or on television due to the interactivity of Websites. As such, web advertisements will be invitations to offer unless it clearly indicates the web advertiser's intends to be bound upon the acceptance. Under the Indian Contract Act, 1872, contracts are binding irrespective of their form. Therefore, unless a specific form is proscribed a contract is binding whether it is oral or in another form. It can be assumed that Electronic Contracts will be valid as under the other form. The Information and Technology Act, 2000 however puts the matter beyond doubt and while adopting the Model Law, states that unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.[126]

3.6.4.1. Offer and Information Technology Act, 2000

Under the Information and Technology Act, 2000, the offer is made, unless otherwise agreed between the originator and the addressee, at the time when the electronic record enters any information system designated by the addressee for the purpose, or, if no system is designated for the purpose, when the electronic record enters the information system of the addressee, or, if an information system has been designated, but the electronic record is sent to some other information system, when the addressee retrieves such electronic record. This reflects the Model Law as to when an offer is made. The Act further provides that an electronic record shall be attributed to the originator if it was sent (a) by originator, or (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record, or (c) by an information system programmed by or on behalf of the originator to operate

---

125 Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

126 *Ibid.*

automatically. This will presumably cover situations when an intelligent `agent' is programmed to issue offers on behalf of an individual. But does not cover a where a file containing the offer is found by another. What would be the motive attributable to the author of the file?[127]

3.6.4.2. Acceptance and Information Technology Act, 2000

Under the Indian Contract Act, 1872, the acceptance of a valid offer results in a valid contract. Such an acceptance may be expressed, in written or oral form or may be implied by the conduct of the offeree. The timing when an acceptance has been made, will depend upon whether the context, inter praesentes (when the contracting parties are face to face with each other) or inter absentees (where the contracting parties are not face to face with each other). Section 4 of Indian Contract Act, 1872 states acceptance is complete as against the offeror, when it is put in the course of transmission; the communication of acceptance is complete as against the offeree, when it reaches the knowledge of offeror. In E-Commerce environment, there are four possible ways to convey acceptance: by sending an e-mail message of acceptance, or by delivery online of an electronic or digital product/service, or by delivery of the physical product, or by any other act or conduct-indicating acceptance of the offer. The Information and Technology Act, 2000 provides that the acceptance is binding on the offeree when the acceptance is out of his control, and binding on the offeror when he receives the acceptance.[128] This differs from the position under the Contract Act. Section 12 of the Act provides for a default acknowledgement process, if the originator and the addressee have not agreed upon the particular method of acknowledgement. It is provided that an acknowledgement may be given by:

- any communication by the addressee (automated or otherwise) or
- any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received

Subsection 12(2) stipulates further,

"Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the

---

127 *Ibid.*
128 *Ibid.*

electronic record shall be deemed to have never been sent by the originator".

As this provision prima facie appears reasonable, but it can lead to unrealistic situations. To illustrate, if A sends a message and insists on an acknowledgement and B responds with an acknowledgement, but with a rider that that acknowledgement must be acknowledged, then A and B may be constantly acknowledging each other's message and may never be able to complete the loop. If one of them does not acknowledge the receipt of the other's message, then the other's message will be deemed as never sent. This may result in the previous message being deemed as never sent, which would affect the earlier message and so on. Thus such legal fiction can create issues that lead to ridiculous situations. It must be noted however, that the provisions of the Information and Technology Act, 2000 requires that they should be interpreted in tune with the provisions regarding the manner in which offers and acceptances are communicated and revoked under the Contract Act.[129]

3.6.4.3. Revocation of Offer and Acceptance and Information Technology Act, 2000

One of the objectives of the Original Information Technology Act, 2000 spelled out in the statement of objects and reasons is to legalize E-Commerce. This objective is reiterated in the objectives of the 2008 amendment to the Information Technology Act, 2000, also. Surprisingly, there was no express provision in the Original Information Technology Act, 2000 validating contracts executed electronically. This lapse was in spite of the fact that there was an express provision to this effect in the Model Law which formed the basis of the Information Technology Act, 2000 as claimed in its statement of objects and reasons. The Information Technology Act, 2000 as amended now in Section 10-A provides that where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the grounds that such electronic form or means was used for that purpose.[130]

---

[129] Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

[130] Farooq Ahmad Mir, " Emerging Legal Issues of E-Commerce in India" 2(2) *International Journal of Electronic Commerce Studies* p.166 (2011).

3.6.4.3.1. Revocation of Offer

Section 5 of the Indian Contract Act, 1872 states that a revocation of offer can be made at any time before the acceptance becomes binding on the offeror. The position under Information and Technology Act, 2000, which is similar to the Model law, states that the offeror is bound by an acceptance when he is in receipt of it. Therefore, if a revocation of the offer enters the information system of the offeree before the offeror is in receipt of the acceptance, the revocation is binding on the offeree and no valid acceptance can be made.

3.6.4.3.2. Revocation of Acceptance

Under principles of contract law, the revocation of acceptance can be made only before the acceptance becomes binding on the offeree, but not afterwards. Section 5 of the Contract Act states that an acceptance may be revoked at any time before the communication of the acceptance is complete as against the acceptor, but not afterwards. The Information and Technology Act, 2000 and Model law differ from the Contract Act and state that an acceptance becomes binding on the offeree the moment the acceptance enters an information system outside the offeree's control.[131]

3.6.5. E-Contract: Incorporation of Terms by Reference

The enormous growth in business has resulted in an impersonal approach to marketing methods facilitated by newer communication methods and necessitated by business convenience. The nineteenth century saw the emergence of standard form contracts, which have been positively received by the courts as a valid means of executing a contractual relationship. It was, however, observed that at times these standard form contracts cause hardship to the weaker party by imposing onerous terms and conditions and thus placing them in a position where they have no choice but to accept them or leave them. These exemption clauses have been regarded as a part of the main contract even if they are not actually mentioned in the main contract, provided they satisfy certain tests evolved by the courts. [132]

---

[131] Subhajit Basu, Richard Jones, "Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000", 17th BILETA Annual Conference Free University, Amsterdam (April 5th-6th, 2002)., *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

[132] Farooq Ahmad Mir, "Emerging Legal Issues of E-Commerce in India" 2(2) *International Journal of Electronic Commerce Studies* p.169 (2011).

Standard form contracts have been recognised by the courts as a valid means of executing contractual relationship. Various rules have been evolved with the passage of time to mitigate the rigour of terms which were considered either harsh to the opposite party or of which the opposite party could not be supposed to have had reasonable notice. Exemption clauses which either limit or exclude liability of the party using the form or impose onerous conditions on the opposite party have been regarded as a part of the main contract even if they are not actually mentioned in the main contract provided they satisfy certain tests evolved by the courts. Web site contracts present a scenario which can be equated to some extent with the challenges posed by the standard contracts at their early stages.[133]

The expression 'incorporation by reference' is used as a concise means of describing the situation where a document refers generically to provisions which are detailed elsewhere, rather than reproducing them in full. Electronic communications are structured in such a way that large numbers of messages are exchanged, with each message containing brief information and relying much more frequently than paper documents on reference to information accessible elsewhere. The question is: are the terms incorporated by reference a part of the main contract and if so under what circumstances? That the terms and conditions which will govern a contract must be brought to the notice of the opposite party is a long established rule.[134]

The Information Technology Act, 2000 does not contain any express provision affording legal status to terms that are not in the main message but are only referred to in that message. There was also no provision in the original UNCITRAL Model Law dealing with this situation. However, the United Nation's Commission on Trade Law, while realizing that by virtue of hyperlinks parties quite frequently provide detailed information not only in the main contents but somewhere else, made an express provision in the Model Law by incorporating Article 5 bis. A similar provision is missing in the Information Technology Act, 2000, which is to be provided by way of amendment. [135]

The courts in India can rely on the rules established for determining the validity of the exemption clauses in standard terms. However, it is to be borne in mind that due to the significant difference in the modes of operation between traditional and

---

133 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* p.152 (2001).

134 *Ibid.*

135 *Supra* note. 134 at p.170.

Electronic Commerce, the traditional tests evolved by the courts in paper-based standard form contracts might be ineffective when applied to corresponding Electronic Commerce terms. It is a long established rule that the terms and conditions that will govern a contract must be brought to the notice of the opposite party. However, when it comes to contracts made electronically, views differ on the best way of achieving this. Thanks to the technology, the options available to bring terms incorporated by reference to the attention of the opposite party are many and varied. It is now possible to design a web page requiring the user to scroll through the terms and conditions incorporated by reference and to confirm that he has not only read those terms but has also accepted them. The courts may consider this as a reasonable mode to bring incorporated terms to the attention of the other party.[136]

3.7. E-Contract: Jurisdictional Issues

An internet contract, is typically a contract that is entered into through the medium of the internet either by using and of the various constructs of the world wide web (such as click wrap contracts) or through the exchange of e-mail stating offer and acceptance of the term and condition of a particular transaction. It is similar to traditional contracts in that it sets out the right and duties, obligations and liabilities of the contracting parties, as well as the services to be rendered and the consideration to be received by the parties. At the same time it is distinct from the traditional concept of contracts in that our understanding of the concepts of offer and acceptance must necessarily undergo a change consistent with the nature of the medium.[137] while an understanding will have to be arrived at with regard to the scope of Jurisdiction of courts in respect of internet contracts.[138]

In the internet both the contract as consent and as contracts as product could be seen. The business-to-business contracts are on the basis of contract as consent. These E-Contracts are formed as an outcome of bargain. Both the parties make these contracts after the approval of the terms and conditions. The only difference between this and the traditional contract is that internet is used as a medium of bargaining.

---

136 Farooq Ahmad Mir, "Emerging Legal Issues of E-Commerce in India" 2(2) *International Journal of Electronic Commerce Studies* p.170 (2011).

137 Rahul Malthan, *The Law Relating to Computers and The Internet* p.11 (Butterworths India, New Delhi, 1st edn.,2000).

138 Tabrez Ahamad, *Cyber Law E-Commerce and M-Commerce* p.266 (A.P.H. Publishing Corporation, 1st edn.,2003).

Most of the business-to-business contracts are of this type. Here both the parties know each other and they confirm the identity of the parties.[139] Through the use of 'digital signature and 'time stamp', the internet does not create any problem in this type of online contract. The parties will be financially stable, they know each other, and the contract is similar to any other ordinary contract. If it is a trans-national contract, it can be resolved through the use of arbitration clause, or any other dispute settlement mechanism, which they choose satisfying the international legal principles regulating trans-national contract. The 'business to consumer' contracts are on the basis contract as a product. Here, the contract comes along with the product in standard terms. The parties in these types of contract are the main victims of the specific characteristics of internet. These types of contract are generally termed as click wrap contracts. They are used for the retail sales on the internet.[140] Once a person enters into a website and wants to purchase some product he has to click on the 'I Agree' button. By clicking on this button he automatically agrees with terms of service, or conditions of use which will have some link from the website. The party may or may not note this but the court has given validity to this contract in *Hotmail Corporation* v. *Van Money pie Inc.*[141] These types of contract can be of many types. One such kind is where the products are advertised in a web page, and the party interested to purchase can do so by paying the money through credit card, or any other means.

The issues of jurisdiction, applicable law and enforcement of the judgments are not confined to only national boundaries. The problems raised are global in nature and need global resolution. An international treaty providing homogeneous rules for governing E-Commerce, between the parties of different countries, on the lines of the instruments already in vogue in Europe, with necessary changes, can provide solution to the present uncertainty. E-commerce is likely to be stifled if the legal environment in which it is to operate is uncertain. The legal position of the businesses using web sites for executing contracts is at present precarious.[142] However, they have various alternatives available to safeguard their interests which include:

---

139 K Vishnu Konoorayar, "Regulating Cyberspace: The Emerging Problems and Challenges" *Cochin University Law Review* (2003)., *available at: http:*//www.ssrn.c.om/ abastract =994574 (last visited on February 6, 2012).

140 *Ibid.*

141 1998 WL 388389(ND Ca., April 20,1998).

142 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* p.163 (2001).

(a) Choice of forum and law: In India parties are free to make a choice of forum by contracting to that effect where two or more courts have jurisdiction. Such that a contract will not be hit by section 28 of the Contract Act which renders agreements in restraint of legal proceedings void. But it is not open to the parties to, by agreement, confer jurisdiction on a court which it does not possess under the Civil Procedure Code. The parties however, do not have choice in case of applicable law because the Central Acts are almost applicable throughout India. This choice of law is available to the parties of different states in America because of the diversity of the state laws and is also available to the parties of different countries in the European Union by virtue of the Rome Convention 1980. [143]

In America, three tests have been laid down to determine the validity of a clause in a contract incorporating choice of law. These are: (a) the chosen law must have a substantial relationship to either party or transaction, (b) the chosen law should not be contrary to the fundamental policy of the legal system which would apply in absence of a choice of law clause, (c) the particular state has a greater interest than the chosen state to determine the relevant issue.[144]

The Rome Convention gives parties of the contracting state a free hand to make a choice of law which will govern their contract. The only requirement is that the choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice, the parties can select the law applicable to the Whole or only to a part of the contract. It is only in the absence of such choice that the contract will be governed by the law of the country with which it is most closely connected. [145]

(b) Conspicuous Notice: Businesses using a web site give notice conspicuously at the beginning of the web page restricting the countries to which web site is directed or indicating the passive or local nature of the web site. This worked well in *Bensusan Restaurant Corp.* v. *King,*[146] Here the New York court held that the state's long arm statutes could not be invoked against a non resident defendant when his business was unquestionably a local operation.

---

143 *Id.* at p.162.

144 *Ibid.*

145 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* p.166 (2001).

146 126 F. 3d 25 (2d cir. 1997).

(c) To provide standard terms and conditions for each country, a task which is nearly impossible.

(d) To use sophisticated filtering techniques to make web access possible only to limited countries.[147] This technique will be acceptable to courts only when it successfully achieves the desired purpose. This is evidenced by the judgment in *New York* v. *World Interactive Gaming Corp.,*[148] where a non resident gaming site was held to have violated the New York state and federal gaming laws when they accepted bets from gamblers in New York, in spite of the address filtering technique used which was intended to prevent access by New York residents. Since this technique could be easily by passed by using the address of other states, the court held that the defendant failed to take technological precautions similar to those taken by other on-line gaming sites. Thus onus lies on the defendant, not only to take technological precautions but those precautions should be sufficient to prevent access to the persons of a country with whom he does not intend to establish contractual relationship.

Conclusion

Electronic Commerce is welcomed throughout the globe due to its ease, flexibility, and speed. The internet has become essentially global in character and it is, therefore, the legal issues raised by its use relating to global ramifications. However, E-Commerce cannot flourish in an uncertain legal environment. It is therefore to formulate due legal principles. The exchange of the information through by electronic means which turns into a contract raises several legal issues which cannot be answered within the existing provisions of the Contract Act. So, there should be either amended the Indian Contract Act or bring a new legislation which was realised by enacting the Information Technology Act, 2000 (hereinafter referred to as IT Act). But the IT Act, 2000 was not a complete code dealing the Electronic Contracts. Hence, the Contract Act is still the fundamental law for contract formation and when the provisions of the Contract Act do not cover any issue raised by the introduction of the information technology, the IT Act, 2000 may be applied.

It is to be noted that there are some principles in the Contract Act which have been changed by the IT Act, 2000 either expressly or by implications. Certainly, there

147 Farooq Ahmad, "Electronic Commerce: An Indian Perspective"9(2) *International Journal of Law and Information Technology* p.163 (2001).

148 No. 404428/98 (Sup. Ct. N.Y. City July 22, 1999).

is nothing about the subject matter of computer-generated agreements under any law present which may render them unenforceable but the laws prevalent did not lays down any express provisions when it came to formation of such contracts. But the some difficulties arise only due to the legal doctrine of contract law which is based on an idealized model of communication between natural persons. Therefore the real issue is to determine how the law should be changed, rather than whether it should be changed. Although the IT Act, 2000 provides for some provisions with respect to the E-Commerce however these provisions are restricted to the legality of the ecommerce and the security of such a transaction only. The Amendment Act of 2008 has tried to bring many changes in the IT Act, 2000 but there are still many gray areas that have to be addressed. The impact of the IT Act, 2000 on the provisions of the Contract Act has to be evaluated. However, when any provisions of the Contract Act are inconsistent with any provisions of the IT Act, 2000 or express provision has been provided in the IT Act, 2000, then only the IT Act, 2000 shall prevail to apply.

It may be debated before the courts which act may be applied either the provisions of the IT Act, 2000 or the Contract Act. There is no indication that the provisions of the IT Act, 2000 modify or change the provisions of the Contract Act so far as Electronic Contracts are concerned except in the preamble where a general statement provides that 'one of the purposes of the IT Act, 2000 is to give legal recognition to the transactions executed by Electronic Data Interchange and other means of electronic communication commonly called as E-Commerce.'

So far as evidentiary value is concerned of the Electronic Contracts that Electronic Contracts are almost same as other hard copy contracts and in case of any discrepancy, there are some prerequisites that fill the lacunae. All Electronic Contracts are valid contracts and enforceable as they are legalized by the Information Technology Act and if there is any infringement with the terms and conditions that one could be made liable. The issue relating to electronic or online contract has become the fundamental forming an e-transaction. As contracts are formed online without human interaction, there is possibility of having been encountered with new problems and grievances. The contract formation issues arise on every time one purchases goods or services online. Purchasers may have question whether a particular advertisement on a vendor's home page constitutes an offer or an invitation to treat; whether the consumer is the offeror or the offeree, when an offer is treated as

accepted. One might assume that the vendor is the offeror, and the purchaser would be the offeree, and accepting to purchase the goods and services under terms dictated by the vendor in the name of standard form contracts and exclusion clauses. There are several questions as to what does constitute consideration, how can be determined the intention of parties and who may enter into an Electronic Contract with validity of digital signature.

The challenges presented by technology to contract law merely involves existing principles suppose to be a case of old wine in new bottles. All forms of E-Contracts must to be made conspicuous to satisfy legal standards of notice of terms. Its binding legal nature should to be impressed upon the end-user, and browse-wrap notices must ideally only be supplemental to a contract that the user has already manifested his assent to. The instantaneous nature of electronic transactions also invites a re-conceptualization of contract formation. E-Contracting has reduced geographical barriers and increases the probability of consumers entering into transnational contracts. This raises some issues relating to private international law and the legal regime here is quite complex and not clear. There is no uniformity since countries started to apply their own domestic laws on jurisdiction, recognition and enforcement, and determination of the applicable law. There should be an International Convention that would provide basis for the development of substantive and procedural aspects of E-Contracts. The issues of jurisdiction at the international level cannot be genuinely resolved by passing national laws. The issue is global in nature and to provide homogeneous rules, a global resolution has to be brought out. An international treaty regarding uniform rules applicable to E-Commerce, jurisdiction of the courts and enforcement of the judgments, needs to be adopted.

CHAPTER IV

E-COMMERCE: CRIME AND JURISDICTIONAL ISSUES IN CYBERSPACE

Introduction

The advancement of digital technology has provided several of opportunities because the Cyberspace provides a medium in which many things can be done in efficient manner. Similarly, the automation of companies, banks, educational institution, and railway reservation are reflections displayed everywhere that manifest dependence of human society on these teeny computers. The advent of digital technology has been a boon to students, lawyers, businessmen, doctors, teachers...and criminals. Unauthorised access and damage to property, theft, and the distribution of obscene and indecent material falls in the cyber crimes as well as has assumed new dimensions with the emergence of the internet. The internet is fast becoming part of life for millions of people. However, it has been transformed into a haven for criminals. India is looking toward the global community. So for as cyberspace is concerned, anonymous servers, hijacked emails and fake websites are being used as a medium for fraud by cyber criminals. Indian fraud on the internet is also a form of cybercrime that has been affected by the global revolution.

Thus, there should be an international cooperation to stamp out such illicit activities and try to protect internet users. Cybercrime is a criminal act that involves computers and networks. Similarly, Cybercrime is a wider term that describes everything from electronic hacking to denial of service attacks that cause e-business websites to lose money. Cybercrimes are criminal activities in which computers, networks or electronic information technology devices are the source, tool, target or place of crime and Cyber crimes are affected by way of illegal access into another's data base, illegal interception, data interference, system interference, misuse of devices, forgery and electronic scams. Paper-based working pattern has become old fashion and outdated because it is unable to keep pace with speedy life of modern world. They have evolved state systems of law and enforcement to deal with the forms of crimes. The internet has become truly mass media. The various kinds of computer and internet related crimes, the most common amongst these are the use of viruses to corrupt and destroy data stored in computers stems. These viruses can be

attached by e-mails, FTPed programme etc. There exist other forms of fraud, robbery and forgery. The main object of the bogus schemes on the internet has to robe a vast amount of money. Through The internet, it is possible to make defamation, assault on a person's character, etc., and the possibilities of a person being caught and held liable are remote. It is, therefore, the growth of crime on the internet directly proportional to the growth of the internet itself, and so is the variety of crimes being committed or attempted.

The internet is the virtual world which is a set of network protocols that has been adopted by a large number of individual networks making the transfer of information among them. The internet helps in communication between users in real space in one jurisdiction with a user in real space in another jurisdiction. Cyberspace means an electronic place where electronic transactions take place and new technology will bring forward a more advanced virtual world. Aim of the analysis is the identification of the jurisdiction versus cyberspace. E-Commerce has become the buzzword in corporate circles.

The page on the World Wide Web can be accessed by web surfers from any state in the nation and perhaps every nation on earth, there arises the issue relating to where exactly a person who has a cause of action, based upon a transaction, may sue. Users and system operators encounter conflicts and seek to resolve disputes, they may take action to establish rules and decide individual cases. Moreover, it is the unique nature of the internet that any given internet transaction will involve parties from more than one jurisdiction. All this provide a new form of law that is a law of cyberspace based on private contracting on a global basis and enforced by a combination of the sysop's ultimate right to banish unruly users and the users' ultimate right to migrate to other online service providers.

In the offline world, disputes are generally resolved through the traditional process of court litigation which is principally based on a territorial basis, i.e., each country has its own laws and courts, which decide disputes falling under their jurisdiction. If the parties to a dispute arising on the internet belong to the same jurisdiction, there is no problem but the dispute in such a case would be resolved in the same manner as any other offline dispute. However, the problem would arise when their customers belong to the different countries and they are transacting with each other through their Web site. This dispute resolution mechanism, based primarily

on territoriality, faces a number of challenges when applied to disputes arising on the internet because The internet is by definition international and can be accessed from almost any place on Earth hence multi-jurisdictional. On the internet, digitized data may have travelled through various countries and different jurisdictions to reach its destination. Additional, the intentional or unintentional violation of trans-boundary laws has become a common occurrence on the internet. Consequently, the redressal of these grievances before the nearest judicial forum, has sparked of the evolution of a new brand of jurisdictional jurisprudence with startling results. As there is little or no proper domestic legislative recognition of the need to evolve a distinct set of regulations for internet jurisdiction, the decisions of various courts of the United States as well as the European Courts, are the only guide to the issues relating to the jurisdiction of courts over the internet.

4.1. Meaning and Concept of Cybercrime

The advent of the computer has been a boon to students, lawyers, businessmen, doctors, teachers and criminals. Unauthorised access and damage to property, theft, and the distribution of obscene and indecent material are all familiar crimes and have assumed new dimensions with the emergence of the internet. The internet is fast becoming a way of life for millions of people. However, it is also being transformed into a haven for criminals. The crime rate on the internet is increasing at rapidly. There have been various kinds of computer and internet related crimes. The most common amongst these is the use of viruses to corrupt and destroy data stored in computer systems. These viruses can be attached to e-mails, File Transfer Protocol programmes, etc. other forms of fraud, robbery, and forgery also exist. Bogus schemes on the internet have robbed many people of a vast amount of money. The internet also makes defamation, assault on a person's character.etc, relatively easier and the possibilities of a person being caught and held liable are remote. In fact, the growth of crime on the internet is directly proportional to the growth of the internet itself, and so is the variety of crimes being committed or attempted.[1]

Since, the internet is composed of computers, crimes occurring on the internet are computer crimes. But, defining a computer crime is difficult. A computer can be the subject of a crime by being stolen or damaged; it can be, the site of a crime (such

[1] See, "Computer and Internet Crimes", *available at:hattp//*:www.cyberspacelaw.com/ crimes. asp (last visited on may 8, 2012).

as fraud or copyright infringement) or it can be the instrument of a crime, such as when it is used to access other machines or store information illegally. These are all computer crimes in the sense that a computer is involved.[2]

The nature of cybercrime depends on a country's socio-cultural environment, technological advancement and geopolitical atmosphere. According to Aguilar-Millan, organized crime involves the illicit flow of goods and services in one direction and the flow of criminal proceeds in the other. Just as the business world has benefited from globalization, so has organized crime. It has also been noted that, in recent years, organized crime groups have committed most of the cybercrimes. From the standpoint of organized criminal groups, a part of the fascinating character of the internet stems from the fact that cyberspace is characterized by less governance and weak rule of law.[3]

The unregulated cyber world offers an opportunity to organized crime groups to mark their victims since their chances of getting caught are few. Organized crime is successful where laws are confusing or when law enforcement is not prepared or structured to retaliate. Both developing and post-communist countries desperately need foreign investment to survive, and if they cannot guarantee investors some protection against fraud, extortion and corruption, the money is likely to be taken elsewhere. When high-risk rates are assigned to a country and huge sums of investment money are diverted to their neighbours, governments react and start taking these issues seriously.[4]

Cyber crime is a subset of computer crime which itself is a subset of the universal set of digital crime.[5]Present scenario of Cyber crimes is summed in the following words: Amidst the surging excitement and interest however, runs a deep thread of ambivalence toward connecting to the internet. The internet's evil twin is the home of Bad Guys - trackers, crackers, snackers, stalkers, phone preaks, and other

---

2 Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.266 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn., 2000).

3 Anjali Kaushik, *Sailing Safe in Cyberspace* p.10 (SAGE Publication Ltd, London,1st edn., 2013)

4 *Ibid.*

5 *Indian Police Journal* p.94 (April-June, 2004).

creepy web crawlers. Business fear that the inforbatin could suddenly veer into the tightway to Hell.[6]

Crime consists of engaging in conduct that has been outlawed by a society because it threatens the society's ability to maintain order. Order cannot exist without rules that proscribe certain harmful activities and institutions that enforce these rules. These rules constitute a society's criminal law. Criminal law is designed to prevent the members of a society from preying on each other in ways that undermine order. It does this by defining certain types of behaviour as intolerable as crimes.[7] Crimes take many forms because each targets a specific harm. Crimes target harming individuals (murder, rape), property (arson, theft), government (obstructing justice, treason), and morality (obscenity, gambling). Because societies have dealt with crime for millennia, they have developed standardized definitions of real-world. Cybercrime also consists of engaging in conduct that is outlawed because it threatens order. Cybercrime differs from crime primarily in the way it is committed. Criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. Cyberspace becomes the tool criminals use to commit old crimes in new ways.[8]

The taxonomy of cybercrimes gives a comprehensive introduction to the term and it is based on such grounds which are commonly seen in the cybercrimes. Some traditional crimes like fraud have taken a new dimension when done online and as they tremendously affect the world economy hence, they come under the category of economy-related crimes. Traditional crimes, like obscenity, take a new form when done online and hence, some writers include it in content-related crimes.[9] Although, the computer world may exist only in intangible form, it affects the physical and real environment. The shift of crime to intangibles has a staggering impact on society, both socially and economically.[10]

---

6 Micheal Rustard andLori E Eisenschmidt, "The Commercial Law of Internet Security" 10(2) *High Technology Law Journal* p.215 (1995).

7 Susan W. Brenner, *Cyber: Criminal Thereats From Cyberspace* p.9 (Pentagon Press, New Delhi, 1st edn., 2012).

8 *Id.* at p.10.

9 *Ibid.*

10 *Ibid.*

4.1.1. Definition of Cyber Crime

The words "cybercrimes" and "computer crimes" are used interchangeably in common parlance. The word "computer crimes" has wider ambit as it entails not only crimes committed on the internet but also offences committed in relation to or with the help of computers.[11] Donn B. Parker distinguishes between the concepts of computer crime and cybercrime, and gives the definitions of the terms in the following words:[12]

1. Computer crime-A crime in which the perpetrator uses special knowledge about computer technology.
2. Cybercrime-A crime in which the perpetrator uses special knowledge of cyberspace.

A computer crime is defined by the US Department of Justice as an illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution.

But the definition is not exhaustive as there are many acts which can be called abusive activities concerning the computer but they are often not clearly illegal. Moreover, most of the cybercrimes are committed via the internet but the definition has no reference to it.[13]

Cybercrimes can be defined as crimes directed at a computer or a computer system but the complex nature of cybercrimes cannot be sufficiently expressed in such simple and limited terms. There are many multilateral organisations recently involved in shaping high-tech crime policy. The Organisation for Economic Co-operation and Development (OECD) has adopted the following definition as the working definition for computer-related crime or computer crime: Computer abuse is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data. [14]

This definition is also deficient as it refers only to the transmission of data while cybercrimes are committed also through transmission of certain malicious

---

11 S.K. Verma, Raman Mittal (eds.), *Legal Dimensions of Cyberspace* p.228 (Indian Law Institute, New Delhi, 2004) .

12 Talat Fatima, *Cyber Crimes* 89 (East Book Company,1st edn.,2011).

13 *Id.* at p.90.

14 *Ibid.*

programs and viruses. Some authorities also use the term "information technology offences" instead of cybercrimes. Thus, it is defined as Information technology offences have been taken to encompass any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer system.[15]

This definition is too wide as it entails any offence where computer or the information stored in the computer is involved in its investigation. It has no reference to certain abuses or security breaches which still do not fall under the term criminal offence. It is given from the viewpoint of the investigator and not from the viewpoint of substantive criminal law which requires a reference to the malicious act or to the guilty mind. Some of the commonly spelt out definitions of cybercrime are: [16]

1. A criminal activity that involves unlawful access to or utilisation of computer systems.
2. Any illegal action in which a computer is used as a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the functions of a computer.
3. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention made or could have made a gain.
4. Any violation of the law in which a computer is the target of or the means for committing crime.
5. Any activity which involves the unauthorised and unlawful access to or utilisation of computer systems or networks in order to tamper with the data, or to intentionally transact anything illegal with the help of computer and the internet, can broadly be called as cybercrime. [17]

All the above definitions are deficient in some important element of cybercrime. All of these have some reference to the computer while only few refer to the internet. Cybercrimes are the products of the internet. A definition of cybercrime is inadequate and unacceptable if it has no reference to the internet. Thus, cybercrimes

---

15 *Ibid.*
16 *Ibid.*
17 *Ibid.*

are the crimes unknown to the legal world prior to the birth of the internet and include not only acts which are employed to commit traditional crimes using the Net but also those crimes which are committed thoroughly and exclusively using the internet. The United Nations highlighted the problem of definition in its manual on the Prevention and Control of Computer-Related Crime stating that although, there is consensus among experts, these definitions have been functional and hence, too specific. A similar problem was expressed by the Council of Europe. The Committee on Crime problems decided to leave out any definition of high-tech crime in the Convention on Cybercrime (2001), allowing individual jurisdictions to apply their own definitions based on their specific body of law. It is, however, interesting to note that the Information Technology Act, 2000 too omits to define cybercrime or computer crime. Even the major cyber laws of the US and the UK do not contain a definition of cybercrime. However, the taxonomy of these elusive crimes would give a circumventing and exhaustive comprehension of cybercrimes. In India, the recent amendment in the Information Technology Act, 2008 has used the term "computer-related offences[18] whereby a good number of cybercrime have been added to the list of crimes already existing.[19]

4.2. Essential Element of Cybercrime

The definition of a crime has always been regarded as a matter of great difficulty. It is a general principle of criminal law that a person may not be convicted of a crime unless the prosecution has proved beyond reasonable doubt that:

- He has caused a certain event, or responsibility is to be attributed to him for the existence of a certain state of affairs, which is forbidden by criminal law; and
- He had a defined state of mind in relation to the causing of the event or the existence of the state of affairs.

Thus, a crime essentially consists of two elements, namely, actus reus and *mens rea*. What will follow will be an analysis of how the theory of criminal law can

[18] By Virtu of Sec.32 of The Information Technology (Amendment) Act ,2008,New Sec.66 is substituted and new Sec. 66(A-F) is inserted in the Information Technology, Act ,2000

[19] Talat Fatima, *op.cit.* p.91.

be applied to internet crimes. For this purpose, hacking, a crime of the internet age, has been used to illustrate the points sought to be made.[20]

In olden days in Europe, during the period of strict liability, severe punishments were inflicted upon the wrongdoer in order to placate the outraged deity[21]. Later, the linking of human behaviour with the harm done replaced the divine link with the harm caused and such responsibility extended even to animals, and inanimate objects like carts, cauldrons, baulks of timber, wheels, boats and the like.[22] Before inflicting some punishment, not only *the actus reus*, but also *the mens rea* with which *the actus reus* is done must be proved beyond doubt. Although D killed P and *actus reus* is done, before D could be punished, the *mens rea* behind it must also be proved.

In *Woolmillgton v. Director of Public Prosecutions*[23], the House of Lords laid that not only the jury is satisfied that D's story is not true but that it should, before passing sentence must be satisfied that D's story of calling it as an accident is "not true" beyond doubt. The English Law of Deodands reflexes such prehistoric practice. In Anglo-Saxon period, it was called brana, the slayer. The couplet depicts the old English rule of criminal liability:

4.2.1. Actus Reus

The word actus connotes a 'deed', a physical result of human conduct. *The actus reus* includes all the elements in the definition of the crime except the accused's mental element. It is not merely an act but may consist in a state of affairs not including an act at all. A well-known definition of *actus reus* is such result of human conduct as the law seeks to prevent.[24]*The actus reus* is made up generally, but not always, of conduct, and sometimes it's consequences and also the circumstances in which the conduct takes place, or which constitute the state of affairs, in so far as they

---

20 Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.269 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn.,2000).

21 J.W.C. Turner, *Kenny's Outlines of Criminal Law* p.7 (University Press, Cambridge, 19th edn., 1966).

22 Nadan Kamath, *op.cit.* p.270.

23 1935 AC 462.

24 J.C. Smith, B. Hogan, *Criminal Law* pp.31-36 (Butterworth and Company Publishers Ltd., London, 6th edn., 1988).

are relevant. Sometimes a particular state of mind on the part of the victim is required by the definition of the crime. If so, that state of mind is a part of *the actus reus*.[25]

Merely guilty intention is not enough to fix criminal liability but some act or omission on the part of the doer is necessary to complete the offence. The actus reus requires proof of an act or omission. The *actus reus* is described as "such result of human conduct as the law seeks to prevent. But "result" is not always equated with actus reus. A dead man with the knife in his back is not the *actus reus* of murder, in fact it is "putting" the knife into his back what constitutes "*actus reus*" causing the murders.[26] There must be a commission or omission to constitute a crime. However, such acts do not incur criminal liability if they are done in a state of automatism like when in sleep, the accused kills someone, sets fire to a house, and causes harm to someone in a state of mental debility, state of intoxication, under anaesthetics or alcohol and hypnotic Influences. To absolve him from criminal liability, the accused must prove that the automatism was not self induced. This mainly applies to crimes of "basic intent". Automatism which is self-induced by other means, may be a defence even to crime of basic intent. Again, a person's conduct may be involuntary due to a mental disease within *McNaughten rules* and in that case, his acquittal is on ground of insanity as different from automatism.[27]

4.2.1.1. Actus Reus in Cyber Crimes

The element of actus reus in internet crimes is relatively easy to identify, but is not always easy to prove. The fact of the occurrence of the act that can be termed as a crime can be said to have taken place when a person is:

- Trying to make a computer function.[28]
- Trying to access data stored on a computer or from a computer which has access to data stored outside[29]

---

25 Thus, in a prosecution for rape the absence of consent on the part of the prosecutrix is an essential constituent of the actus reus. If the prosecution fails to prove such absence of consent the actus reus is not proved and the prosecution must fail. See. Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.269 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn.,2000).

26 J.C. Smith, B. Hogan, *Criminal Law* p.33 (Butterworth and Company Publishers Ltd., London, 6th edn., 1988).

27 Talat Fatima, *op.cit.* p.65.

28 This is done by using input devices like the key board mouse, etc.

- If he or she uses the internet to attempt to gain access, signals pass through various computers. Each of these computers is made to perform a function on the instruction which the person gave to the first computer in the chain. Each such function can be said to constitute *actus reus*. [30]

- Attempting to login, even if those attempts fail. This is because most hackers have an automated system of trying passwords, the very running of which can be considered to be a function being performed.[31]

Actus reus in cybercrimes has become a challenge as the entire act is committed in intangible surroundings. The perpetrator may leave some footmarks in the machine itself though it becomes a herculean task for the law-enforcers to prove it in the law courts as, it is required to be in physical form or at least in such a form where it becomes admissible in evidence. Every time a computer is moved by a human hand, any of the following actions may follow which are commonly regarded as actus reus.

1. Trying to do some act using the computer.
2. Either attempting to access data stored on a computer or from outside through the said computer

---

[29] A hacker uses an authorised person's password to login to any company's main server, hoping to gain access to the company's customer details, the computer to which he logs in to stores these details in a huge data storage unit, which is located elsewhere. The data itself is stored on a magnetic tape. The processing unit of the computer retrieves this information from the storage unit. The computer would be thought to include the magnetic tape, and so the data would still be considered as being held in a computer. See, C. Gringras, *The Law of The Internet* p.216 (Butterworths, London,1st edn., 1997).

[30] For example, a hacker uses his computer to access an unauthorised account at an Internet Service Provider (ISP). It is enough for the prosecution to prove that either of the computers is belonging to the hacker or the Internet Service Provider were made to function. However, the prosecution would choose to prove that the Internet Service Provider's computer was made to function only when it is not possible or extremely difficult to prove that the hacker's computer was made to function. In such a case it will be difficult for the prosecution to prove that the functioning of the Internet Service Provider's computer was a result of the instructions given by the hacker unless there is other evidence to prove the same.

[31] A hacker oversees a password being entered by someone logging in to a remote computer. The login prompt specifies that the user must be authorised to access the computer. Later, the hacker attempts to use the password himself, but fails owing to the remote computer allowing only one login each day. This would still be actus reus as the rejection itself constitutes a function and this function was caused by the hacker using the password without authorisation at the wrong time.

3. Every time the computer is used by its user while gaining access, signals pass through various computers which are made to perform some function when the command given by the user pass through it. Each such function falls under the term *actus reus*.

4.2.2. Mens Rea

The second essential constituent of a crime is what is often called a guilty mind, also known as *mens rea*. Until the 12th century, a man could be held liable for a harm simply because his conduct caused it, without proof of any blameworthy state of mind, whatsoever, on his part. However, this interpretation underwent a gradual change until modem Common Law came to regard a guilty mind of some kind or some other such mental element as always being necessary.[32]

Mens rea may comprise a number of different mental attitudes including intention, recklessness and negligence. Intention refers to the state of mind of a man who not only foresees but also wills the possible consequences of his conduct. There cannot be intention unless there is foresight, since a man who intends a particular act must have reasonable foresight of the consequences of such act. Though intention cannot exist without foresight, the converse is not necessarily true, i.e., there can be foresight without intention. A person who does not intend to cause a harmful result may take an unjustifiable risk of causing it. If a man foresees the possible or even probable consequences of his conduct and yet, without desiring them, still persists with such conduct, he knowingly runs the risk of bringing about the unwished result. Such conduct may be defined as recklessness. [33]

Finally, a man may bring about an event without having any intention or foresight. He may never have considered the possible consequences of his conduct and the end result may come as a surprise even to him. Under Common Law, there is no criminal liability for harm caused by one's inadvertent or unintended and unforeseen conduct.[34]

---

32 Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.270 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn.,2000).

33 *Ibid.*

34 *Id.* at p.271.

2.2.1. Mens Rea in cybercrimes

An essential ingredient for determining *Mens rea* on the part of the offender is that he or she must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorised. There must be, on the part of the hacker, intention to secure access, though this intention can be directed at any computer and not at a particular computer. Thus, the hacker needs not be aware of which computer exactly he or she was attacking. Further, this intention to secure access also need not be directed at any particular or particular kind of, programme or data.[35] It is enough that the hacker intended to secure access to programmes or data per section 18 of Information Technology Act, 2000.

Thus, there are two vital ingredients for *mens rea* to be applied to a hacker:

- The access intended to be secured must have been unauthorised; and
- The hacker should have been aware of the same at the time he or she tried to secure the access.

The second ingredient is easier to prove if the accused hacker is a person from outside who has no authority whatsoever to access the data stored in the computer or the computers; however, it is difficult to prove the same in the case of a hacker with limited authority.[36] *Mens rea* has come to be recognised as an essential element of crime except in statutory offences where liability is strict. With the advent of e-crimes, the legal world faces the difficulty, besides many others to pinpoint *mens rea* in cybercrimes. In cybercrimes, one should see what the state of mind of a hacker was and that the hacker knew that the access was unauthorised. Thus, a "particular computer" need not be intended by a hacker, it is enough if the unauthorised access was to "any computer".

Thus, following two ingredients form the *mens rea* applied to a hacker:[37]

1. The access intended to be secured must have been unauthorised.
2. There should be awareness on the part-of the hacker regarding the access.

---

35 *Id.* at p.272.
36 *Ibid.*
37 Talat Fatima, *Cyber Crimes* p.67 (East Book Company,1st edn.,2011).

Awareness on the part of the hacker becomes easier to prove where he is an outsider and has no authority to access. But where a hacker already has limited authority as in the case of the employee of a company, it becomes difficult to establish that he exceeded his limits and was even aware of the fact that he is exceeding it.[38]

4.3. Classification of Internet Crimes

Cyber crimes have been classified on the basis of nature and purpose of the offence and have been broadly grouped into three categories depending upon the target of crime. It may be against person, property, or government. The cyber crimes against person include crimes like hate messages, stalking, defamation and transmission of pornographic material. Cyber Crimes involving property includes unauthorized computer trespass, vandalism and transmission of harmful programmes unauthorized possession of computerized information. Third category of cyber crimes is more popular called as Cyber-terrorism.[39]

The most comprehensive classification of computer crimes has been given by David Carter who classified computer-related crimes into the following three broad categories:

(a) Where computer is the target of the crime, e.g. theft of data/information, theft of intellectual property such as computer software, unlawful access to criminal justice and government record etc.

(b) Where computer facilitates the commission of crime e.g. fraudulent use of Automated Teller Machine (ATM) Card, Credit Card frauds, telecommunication frauds, frauds involving stock transfer etc.; and

(c) Whether computer is incidental to the crime e.g. these crimes can be divided into two broad categories:

I. Internet Crimes - such as theft of information, theft of passwords, espionage, spamming, launch of malicious programmes etc.; and

II. Web based crimes such as web sites based programmes, crimes through e-mail, use net related crimes, internet relay chat crime etc.[40]

---

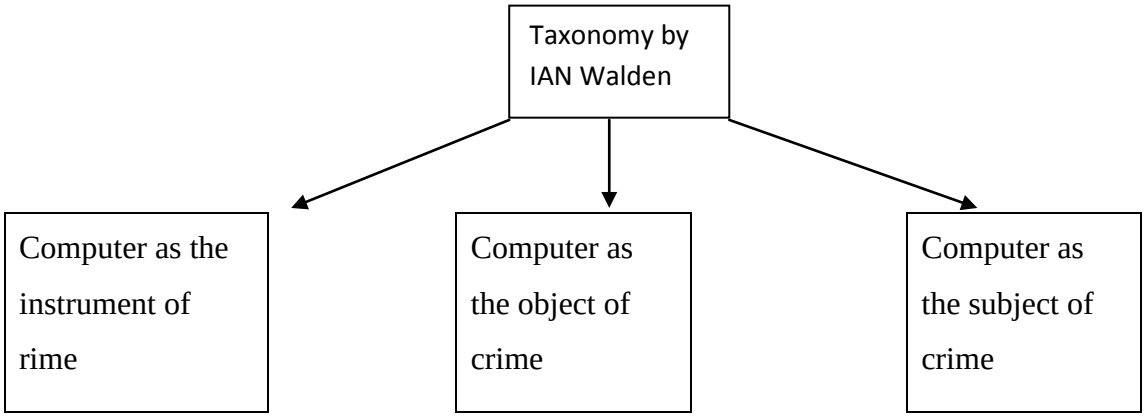
38 *Id.* at p.68.

39 Arti Dubey, *Cyber Law and Terrorism* p.38 (National Conference on Cyber Laws and Legal Education, NALSAR University of Law, 2000).

40 Subhas P. Rathore, Bharat B. Das, Cyber *Crimes: The Emerging Trends and Challenges* pp.55-67 (National Conference on Cyber Laws and Legal Education, NALSAR University of Law 2001).

Cybercrimes have taken two dimensions. Firstly, crimes which attack at computer system itself. These are committed through data manipulations like: Data Diddling, IP Spoofing, Masquerading, etc. using techniques like Logic bomb, Trojan horse, Salami, etc. Such crimes encircle the entire globe and the modus operandi is purely technical and sophisticated, posing serious threat for law-enforcing agencies. International protocols create a new category of irregularities unknown to the society prior to the internet. These are theft of internet hours, internet services and informational harms including dissemination of unwanted information on the Net, etc. Secondly, computer crimes have facilitated traditional crimes like murder, fraud, defamation, pornography, etc. The American Congress in its session, while passing a Bill on digital telephony in 1993, said:

The communication systems and networks are often used in the furtherance of criminal activities including organized crime, racketeering, extortion, kidnapping, espionage, terrorism and trafficking in illegal drugs. The complex nature of cybercrimes is understood by various thinkers in varied manner. While all of them recognise the role of computer in the commission of cybercrimes, their categorisation differs. Ian Walden gives three categories of cybercrimes as regarding the role of computers. He says, the computer may constitute the instrument of the crime, such as in murder and fraud, the object of the crime such as the theft of the processor chips, or the subject of the crime such as hacking and distributing viruses.



Taxonomy by Ian walden

Walden refers to some of the offences of English criminal law where there is involvement of computers.

The first category of such crimes is traditional crimes that are committed by using the computer, like fraud, and which are referred to as computer-related crimes.

The second category concerns content-related crimes which involves intellectual property and pornography.

The third category is offences that have been established specifically to address activities that attack the integrity of computer and communication systems referred to as *computer integrity offences.* These are the typical forms of high-tech crimes. A further authority gives two categories of cybercrimes in the following words:

It has two main categories: In the first, the computer is a tool of crime, such as fraud, embezzlement and theft of property or is used to plan or manage a crime.

In the second, the computer is the object of crime such as sabotage, theft or alteration of stored data or theft of its services. In this category, data may represent money directly as in the electronic fund transfer systems or indirectly, as in the cost of replacing erased or altered data, or the losses incurred if the data are disclosed or used without authorization. Thus, underlying the definition of computer crime is the concept that data represents money. Although, the computer may be used as a tool or as the object in these crimes, it is the people and not computers who commit these offences. The computer cannot be manipulated without the instruction of a human being. Consequently, a comparative study of typology of cybercrimes given by various writers and authorities reveals that the computer network rather than a stand-alone computer is the major factor in the commission of cybercrimes. All the major legal complexities arise when a crime is committed in the virtual world or via the internet. Traditional crimes when committed with the aid of computers is not as formidable a challenge as when hitherto unknown harmful activities take the form of crimes in an intangible environment and pose a threat to law. [41] The following taxonomy, mainly inspired by the taxonomy given by the Cybercrime Convention, 2001 thus, conveniently includes the major harmful activities, which are, from the viewpoint of legal

[41] Talat Fatima, *Cyber Crimes* p. 97 (East Book Company,1st edn.,2011).

procedures like investigation, prosecution, production of evidence and jurisdiction, posing new challenges to the criminal legal system the world over.[42]

4.3.1. Cybercrime: Economy-Related Offences

Perhaps economy is the worst casualty of internet vandalism. So, powerful is the impact of the network technology on the economic world and so great is its speed that an oft-quoted estimate is that UK's currency reserves could be transferred abroad in 15 minutes. In the last few decades, Electronic Commerce has become a major buzzword in the information society. The UK Department of Trade and Industry defines the E-Commerce concept as follows "*using an electronic network to simplify and speed up all stages of the business process, from design and making, to buying, selling and delivering*." E-Commerce is not a new phenomenon with related activities like Electronic Data Interchange (EDI) having occurred since 1970. But at that time, it was essentially business-to-business transaction occurring in a closed environment. The internet has now made E-Commerce services directly available to common man and it is usually referred to as B to C or business-to-consumer E-Commerce. It is said that the internet for its speed, reasonable reliability, cost effectiveness and globally accessible quality, has become the first preference of businesses. Not only that a wide variety of goods are shown on the Net for a better choice but today sites like amazon.com and eBay.com are more useful and practical.[43]The focus here is mainly on those economic crimes which frequently abound the cyberspace and cause formidable financial losses.[44]

4.3.1.1 Fraud

Jack Blum says that International fraud, commercial fraud, money laundering and tax evasion will be the most important enterprise crimes of the future. With new technologies, the inherent weakness of established systems is getting exposed, for example, the credit card frauds are mounting. Magnetic strip is easily reproduced. VISA and Mastercard companies are losing about US $5 billion annually for their old

---

42 *Id.* at p.99.
43 *Id.* at p.100.
44 *Ibid.*.

technology.[45] Thus, for the commission of the offence of fraud, it is a requirement to show that a person has been deceived.[46]

Here there is intention to defraud but there is no destruction of any computer resource or data. Section 65 of Information technology act, 2000 (hereinafter referred to as IT Act) deals with tampering with computer source documents which is again not applicable to A as here A's case does not show tampering with "computer source code". Section 66 of the unamended IT Act had mainly dealt with "hacking with computer system". Under the IT (Amendment) Act, 2008 (ID of 2009), Section 66 read with Section 43(i) reveals that to commit an offence under it, one has to prove that the act of intrusion into any computer data was done dishonestly and fraudulently. Thus, an equivalent of Section 415 Indian Penal Code is yet to be found in the IT Act.[47]

An important ingredient of such an intent, as is clear from the above discussion is to show an accrual of some advantage (which may not necessarily be pecuniary) to the author of such a deception. Now forgetting for a moment that the entire activity is carried out without the internet medium, i.e. in real life situation, then what is the law which will be applied to A? The first provision which comes to one's mind is Section 415[48] Indian Penal Code which defines the offence of cheating. Thus, A, if he is in real life situation, sends a letter to X or promises X to send goods, knowing fairly well at the time of making the promise that the money which is being taken in advance for the curio items to be sent, will never be sent, then he clearly

---

45 Satya Pal Singh, "Economic Crimes: Key Issues" *The Indian Police Journal* p.48 (January-March 2001).

46 Talat Fatima,*op.cit.* p.101.

47 Talat Fatima, *Cyber Crimes* p.101 (East Book Company,1st edn.,2011).

48 See, Sec.415 of the Indian Penal Code,1860, elaborates: Whoever, by deceiving any person, fraudulently or dishonestly, induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".
Explanation-A dishonest concealment of facts is a deception within the meaning of this section.

cheats. A cheats X and is guilty under Section 417.[49] This is further, explained by the following illustrations pertaining to Section 415:

(a) A intentionally deceives Z into a belief that A means to repay any money that Z may lend him and thereby, dishonestly induces Z to lend him money, A not intending to repay it. A cheats.

(b) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby, dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards, breaks his contract and does not deliver it, he does not cheat, but is liable only to a civil action for breach of contract.[50]

Thus, in the above situation, A will be held guilty under Section 415. It is to be noted that A uses the electronic communication and, though Section 415 is applied to him as he has the intent to deceive and also intends to gain advantage (using the internet means), namely, the money which will be received by A, conditions under Section 66, read with Section 43(i) are not satisfied. Here, if Section 66 read with Section 43(i) as amended by the of the IT (Amendment) Act, 2008 is applied, the main difficulty that arises in fixing A's liability is that Section 43(i) requires causing damage to computer or data, etc. to render A liable, which is not the case here.

The opening words of Section 43 say that "*if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network does any of the acts enumerated from sub-sections (a)-(i) then he is liable to pay damages by way of compensation to the person so affected."* In Section 65, the intention is to conceal or destroy or alter the computer source document and in Section 66, the acts under Section 43 should be done dishonestly or fraudulently to attract the punishment whereas purely for the offence of fraud, an element of deceit accompanied with a hope to gain advantage through internet means for the author of the deceit is necessary, which is not found in any of the three sections of the IT Act, 2000 enumerated above. [51] As the Indian Penal Code is a traditional law, an

---

[49] See, Sec.417 of the Indian Penal Code,1860, enumerates the punishment for cheating: Whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both (IPC).

[50] Talat Fatima, *Cyber Crimes* p.107 (East Book Company,1st edn.,2011).

[51] *Id.* at p.108.

amendment is suggested in Section 415 and it is recommended to bring it on the lines of the US law where the use of interstate wire communications is included as one of the ingredients of fraud committed via the internet. After the amendment, Section 415 should read as this: "*Whoever, by deceiving any person, fraudulently or dishonestly, by electronic communication or otherwise, induces*."

Section 415 of the Indian Penal Code can then be independently applied to the internet fraud where there has been no concomitant computer intrusion. However, in cases where fraud is committed by vandalising the communication system and by infusing malicious programs and codes, Section 415 of the Indian Penal Code read with Sections 43, 65 or 66, whatever the case may be, can be applied.[52]

4.3.1.2. Forgery

Online forgery is an offence which needs little effort as compared to offline forgery. The online trading has opened new and easier ways to forge, the originality and individuality of an artist or a poet is effortlessly forged, whether it is an autographed poem of John Lennon or a baseball signed by Mother Teresa. Forgery is an offence which existed much before the internet and in common law. It is defined as fraudulent making or alteration of writing to the prejudice of another man's right. Computer forgery is the alteration of computerised documents. Since, the proliferation of high-resolution computerised colour laser copiers, a new generation of fraudulent counterfeiting has emerged. These copiers can modify existing documents, the quality of which is indistinguishable from the original without referring to an expert for analysis. The perpetrators can even create false documents without the necessity of referring to an original document. Since, everyday human living has become used to vary forms of documents and since property entitlement, money transaction, businesses and in fact every facet of human life is dependent on documents, their value in the eyes of the criminal is no less. The hitherto paper heritage has now also become part of the intangible documentation of files. In fact, many original files are prepared through the electronic medium. As is their value, so is their attraction for the criminal. He is using it on a mass scale for nefarious purposes, even for committing the traditional crime and uses the computer for forgery of signatures on a number of documents where the signatures show the perfect replica not of the original only but also of another inter se and there are no dot or dash lost, no stroke with different bend,

[52] Talat Fatima, *op.cit.* p.110.

kinks or angulations, no natural variation and it appears to be an impossible task for a human being. Current software-based products for digital manipulation provide a powerful tool for even the most amateur of forgers.

In India too, forgery is an offence defined as the making of a false document with anyone or more of the intents mentioned in Section 463of the Indian Penal Code (hereinafter referred to as IPC). The traditional offence has a reference to document or part of a document in the said section. The technological boom and the instances of forgery through computer rendered the said section inadequate for the purposes of digital forgery as the term document could not be applied to computer data and information stored therein which was transient in nature. It was thus thought necessary to make the traditional legal provision regarding forgery workable and hence, certain amendments were made in the IPC. These amendments made electronic record as also an instrument of the offence of forgery. The relevant section is thus,

> **470. Forged** "*(document or electronic record)-A false (document or electronic record) made wholly or in part by forgery is designated 'as forged (document or electronic record)*".

Thus, now not only paper document but an electronic record which is intangible in nature can be the object of forgery. The IT Act, 2000 has left unchanged the definition of the tradition offence of forgery but has added "electronic record" as the object of the crime. The amended Section 463 defining the offence of forgery stands thus,

> **463. Forgery** –"*Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery*".

This definition after the amendment includes "the making of any false electronic record or part thereof with intent to cause damage or injury to the public or to any person". Traditionally speaking, the offence of forgery is said to be committed when the maker of it knows that the document is not genuine but represents it as genuine with the object of defrauding someone. When such false making is done through using the digital means such as desktop publishing systems, colour laser and inkjet printers, colour copiers, and image scanners which enable crooks to make fake,

with relative ease, cheques, currencies, passports, visas, birth certificates, ID cards, etc.[53] The amended Section 464 IPC runs thus,

> **464. Making a false document**.-"*A person is said to make a false document or false electronic record-*
>
> *First-Who dishonestly or fraudulently-*
>
> *(a) makes, signs, seals or executes a document or part of a document;*
> *(b) makes or transmits any electronic record or part of any electronic record;*
> *(c) affixes any (electronic signature) on any electronic record;*
>
> *(d) makes any mark denoting the execution of a document or the authenticity of the (electronic signature), with the intention of causing it to be believed that such document or part of document, electronic record or electronic signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or*
>
> *Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with electronic signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or*
>
> *Thirdly-Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his electronic signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents- of the document or electronic record or the nature of the alteration"*.[54]

Thus, the section comprehensively covers the case of digital forgery where it also clarifies in Explanation 3, that the expression affixing electronic signature shall have the same meaning as it appears in Section 2(1)(d) of the IT Act, 2000. The effect of technology on the offence of forgery has been tremendous as computer technology by its very nature reduces the burden of handwritten documents and simplifies the job of a writer. Mass copying which hardly can be termed as copy requires nanoseconds and the identical replica of the original makes the job of a law-enforcer a challenging one.

---

53 *Id.* at p.113.
54 *Id.* at p.114.

4.3.2. Cybercrime: Computer-Related Offences

Some cybercrimes existed before the emergence of the computer. The computer only provided a new tool by which a crime could be perpetrated. Examples of this type are identity theft, fraud and cyber espionage.

4.3.2.1. Theft

Cyber fraud implies illegal access to a computer system, illegal data acquisition and misleading information. Illegal data acquisition is very often not criminalized because older regional and international legal frameworks do not contain provisions for it. Misleading information includes information that is listed in search engines and can influence consumers and business partners in their decisions. A mere posting that an E-Commerce company is involved in fraudulent activities can, for example, negatively influence the sales of an online store. Cybercriminals set up websites to manipulate search engines and then charge companies to remove the postings. Financial theft and misuse committed using computers are the most frequent crimes and they include misuse of credit cards and making unauthorized financial transactions. Cyber theft and fraud may be of different kinds. The theft of a customer's credit- or debit-card information, automated teller machine (ATM) frauds, financial data theft, identity theft and mobile frauds are major ones in the financial fraud category. Technological development today enables digitalization and the alteration of contents of various kinds of paperwork and documents, which are used in legal traffic, and forgery of data in its electronic form.[55]

4.3.2.1. Hacktivism (Hack + Activism)

Hacktivism refers to the use of computers and computer networks as a means of protest to promote political ends. These tools include website defacement, redirection, denialof service attack, information theft and so on. Hacktivism can be understood as the writing of code to promote a political ideology: promoting expressive politics, free speech, human rights and information ethics through software development. Acts of hacktivism are carried out in the belief that a proper use of code will be able to produce results similar to those produced by regular activism or civil disobedience. Hacktivist activities span many political ideals and issues. Hacktivists

---

[55] Anjali Kaushik, *Sailing Safe in Cyberspace* p.32 (SAGE Publication Ltd, London,1st edn.,2013).

believe in translating political and ideological thought into code. This means anyone should be able to write a code and express himself. With access to data and activism surrounding this term and the emergence of wikileaks and the hacktivism group, Anonymous, it is difficult to ignore this phenomenon. Simultaneously, the boundary between hacktivism and cyber warfare continues to blur. Recently, the group Anonymous launched several, major, distributed DDoS attacks against websites of copyright protection societies and adult film industries such as SGAE (Spanish agency) and HADOPI (French government agency).[56]

In November 2010, the WikiLeaks disclosure of more than 250,000 diplomatic cables of the United States State Department upset many people. WikiLeaks, as well as its supporters and detractors, were victims of numerous DDoS attacks from people supporting one of the two camps. Also in November 2010, Phayul.com, a leading news portal of the Tibetan diaspora, was victimized by a DDoS attack that rendered the website slow or inaccessible.[57]

4.3.2.3. Cyber Espionage

Corporate espionage has been recognized as a crime under existing criminal laws. The computer and the internet are new tools for espionage. An instance of how they may be used is explained when one comprehends the ease with which industrial secrets, copyrights and patented information may be downloaded and sent over the internet to a competitor. This has the potential to cause huge damage. An innovation, which is yet to hit the market, may be stolen and exploited. It may even be sold for huge sums of money. Networks and connectivity only make it simpler. According to Schiller, Cyber spying or cyber espionage is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on the internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.[58]

---

56 *Id.* at p.33.
57 *Ibid.*
58 *Ibid.*

4.3.2.4. Exposure to Indecent Content

Other related crimes include polluting the youth through exposure to indecent content and luring young children to reveal details through social networking sites. Such activities have a lot of financial gain associated with them. Distribution of indecent content is the most under-prosecuted crime today. The regulation in this area is also insufficient.[59]

4.3.2.5. Forgery

Information technology has eased the process of forging while simultaneously making the act extremely hard to discover. This is very good news for forgers but it makes the lives of law-enforcement officers difficult. Apart from classic forgery under the existing legal systems, there may be many new challenges. Can illicit use of a password be criminalized as forgery? Will creating an electronic signal be deemed forgery? The last challenge is that, in many legal systems, there is a 'person' to be deloused. In this case, how would forgery be purported to induce a computer system or a network? Embezzlement is the most common example in this category. It is a kind of financial forgery by a person to whom property has been entrusted. Countries with high financial traffic are more affected with this type of cybercrime. In the United States, embezzlement is a statutory offence.[60]

4.3.2.6. Cyber Terrorism

Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. It is the use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. Cyberterrorism is defined by the Technolytics Institute as 'the premeditated use of disruptive activities, or the threat thereof, against computers and or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives. The term was coined by Barry C. Collin in the 1980s. Cyberterrorism means attacks on computers and internet resources from an

---

59 *Ibid.*
60 *Ibid.*

ideological motivation rather than an economic one. When such a crime is perpetrated purely from an economic motivation, it is termed cybercrime. Cyberterrorism may include DDoS attacks against government websites and service networks, such as power distribution, banking, public delivery services, and so on. It may be used by individuals and groups to threaten governments and to terrorize the citizens of a country.[61]

The internet is often used as a tool for cyberterrorism in countries having problems with each other, such as Taiwan and China, Israel and Palestine, India and Pakistan, China and the United States, and many other countries. The National Conference of State Legislatures (USA) defines cyber terrorism as the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples of cyber terrorism include hacking into computer systems, introducing viruses into vulnerable networks, website defacing, denial-of-service attacks and terrorist threats made via electronic communication. This transformation in the methods of terrorism from traditional to electronic methods is one of the biggest challenges faced by modern societies. A consolidated effort is needed in terms of awareness building at each level (individual, regional, national: international), as well as support of laws and regulations and international cooperation to tackle the problem of cyberterrorism and cover its various forms. Cyberterrorism is one of the biggest threats of our times and unless individuals, governments and nations cooperate.[62]

The Stuxnet worm is the latest example of cyberterrorism attacks. It targeted programmable logic controllers (hereinafter referred to as PLCs) that are used in the industrial control systems (hereinafter referred to as ICS). The main purpose of ICS is to regulate the flow, or move the actuators as in a typical chemical plant scenario. The worm targeted specific manufacturer PLCs and it could reprogram them by injecting a malicious code. This at a ground level is very dangerous because industrial systems are the potential targets. The attacks were specific to manufacturers and nuclear power plants of a country. This requires specific knowledge of the technical aspects of

---

61 *Ibid.*

62 *Id.* at p.36.

the hardware used and this makes sceptics wonder about the involvement of governments in funding the development and propagation of Stuxnet. Cyberterrorists are greatly interested in gaining publicity in any possible way.[63]

For example, information warfare techniques like Trojan horse viruses and network worms are often used to not only do damage to computing resources, but also as a way for the designer of the viruses to 'show off'. This is a serious ethical issue because many people are affected by these viruses and worms. For one, the viruses can consume system resources until networks become useless, costing company's lots of time and money. Also, depending on the type of work done on the affected computers, the damage to the beneficiaries of that work could be lethal. Even if the person did not mean to harm someone with their virus, it could have unpredictable effects that could have terrible results. Terrorists can communicate, advertise and even conduct their operations online. Our existing legal systems may be able to comprehend these operations in many cases, but certain amendments may be required. Cyberterrorism can be used for religiously motivated issues, such as the Israel-Palestine conflict and the Arab-Iranian dispute or even the Islamic versus the American and European ideological and thought processes. [64]

4.3.3. Cybercrime: Content-Related Offences

The data which is processed by computers is often much more valuable than the hardware itself. That is why crimes committed against the content of those computers are of great importance.

4.3.3. 1. Copyright

In many existing laws, information is protected in relation to know-how, trade secrets and against stealing intellectual property rights (IPRs). However, in the case of cybercrimes, information itself may be a product and therefore, require protection. Copyright issues include the unauthorized copying of computer software (often referred to as software piracy), which is a copyright infringement of software. Most countries have copyright laws which apply to software, but the degree of enforcement

63 *Id.* at p.37.
64 *Ibid*.

varies. Copyright authorization needs to be checked carefully before downloading, uploading or distributing material over the internet. [65]

The motivations for copyright infringement may vary across individuals and geographies. It includes reasons such as pricing-unwillingness or inability to pay the price asked by legitimate sellers, unavailability and geographical restrictions on online distribution and international shipping of software. A user can share a file with other users, which they can download through the internet. However, this may result in infringement of copyright. In the case of music and movies, this sharing may often be illegal. The regulation of files shared and copied through the network is not clear. The copyright laws of one country may be difficult to enforce outside the country. It is seen that countries where enforcement is poor host file-sharing software. This software may be used by cybercriminals to distribute files in countries where laws are more stringent. In such cases, enforcement becomes difficult. For example, the program Kazaa is owned by the Australian company Sharman Holdings. Incorporated in Vanuatu it was developed by two Dutch software engineers. The online index of bit torrents The Pirate Bay is hosted in Sweden with backup servers in Russia. [66]

4.3.3. 2.Stalking, Harassment, Hate Speech

Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant message (IM), or messages posted to a website or a discussion group . A cyberstalker relies upon the anonymity enabled by the internet to allow him to stalk his victim without being detected. Cyberstalking messages differ from ordinary spam in that a cyberstalker targets a specific victim with frequent and threatening messages, while the spammer targets a multitude of recipients with simply annoying messages. Stalking has typically been defined as involving repeated harassing or threatening behaviour. The goal of the traditional stalker is to exert control by instilling fear into the victim. While cyber bullying and cyber harassment may damage an individual's reputation or livelihood, cyber stalking is more likely to result in severe and immediate emotional or physical harm. [67]

---

65 *Ibid.*
66 *Id.* at p.38.
67 *Ibid.*

Stalking and harassment are malicious activities directed at a particular person. They may or may not be deemed criminal activities, depending on the jurisdiction. But when these activities are committed via computers, all jurisdictions may not be able to prosecute them. In India, such issues are covered under Sections 66 and 67 of the Information Technology Act, 2000.[68]

In the case, *Shreya Singhal* v. *Union of India*[69] the Supreme Court held that Section 66A[70] of the IT Act, 2000 was struck down and was not saved by Article 19(2) of the Constitution on account of the expressions used in the section, such as "annoying," "grossly offensive," "menacing,", "causing annoyance." Apart from not falling within any of the categories for which speech may be restricted, Section 66Awas struck down on the grounds of vagueness, over-breadth and chilling effect. When it comes to regulating speech in the interest of public order, the Court distinguished between discussion, advocacy and incitement. It considered the first two to fall under the freedom of speech and expression granted under Article 19(1)(a) of the constitution of India, and held that it was only incitement that attracted Article 19(2) of the constitution of India.

The Supreme Court has wisely put an end to private adjudication of lawfulness. Section 79(3)(b) the IT Act, 2000 and Rule 3(4) have been read down to mean that the intermediary must have actual knowledge of a court order or

---

68 Anjali Kaushik, *Sailing Safe in Cyberspace* p.39 (SAGE Publication Ltd, London,1st edn.,2013).

69 Writ Petition (Criminal) No.167 of 2012 held on March 24, 2015.

70 **66-A of the Information Technology Act, 2000:**
Any person who sends, by means of a computer resource or a communication device,—
(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
shall be punishable with imprisonment for a term which may extend to three years and with fine.
Explanation.— For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

government notification. Even if an intermediary chooses not to act in response to a private takedown notice, it will retain its immunity under Section 79 the IT Act, 2000.

Section 79 the IT Act, 2000 and the intermediary as a judge Section 79 the IT Act, 2000 provides a safe harbour for intermediaries: if they abide by the requirements of Section 79(2), they retain immunity. But, under Section 79(3)(b), intermediaries can lose their immunity from prosecution if, after receiving a takedown notice, they do not take down content in three circumstances: (1) if they have actual knowledge that third-party information within their control is being used to commit an unlawful act (i.e., by suo moto deciding the lawfulness of content); (2) if a court order requires takedown of content; (3) if a government notification requires takedown. Rule 3(4) of the Intermediaries Guidelines Rules, 2011 has a similar provision.

Section 69A the IT Act, 2000 empowers the government and its agencies to block websites on any of six grounds: "in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above". The blocking procedure is set out in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. It requires that a Committee for Examination of Request (CER) examines each blocking request, and gives the content-generator or host 48 hours to make a representation. The Secretary of the Department of Electronics and Information Technology then issues the blocking direction to the intermediary. However, the court has recognised and upheld the rights of viewers, readers and listeners in its decision on Section 66A the IT Act, 2000, it failed to consider the impact of Section 69A and its Rules on readers and listeners. Our free speech rights as listeners are equally affected when legitimate websites containing information are blocked. Transparency, block page notifications and judicial review are essential to determine whether each blocking direction is valid.

In this case, *Dr. Prakash Vs. State of Tamil Nadu and Ors.* [71] Supreme court observed that the petitioner was a remand prisoner in of Vadapalani Police Station, he was detained under Section 3(1) of the Tamil Nadu Preventive Detention of Bootleggers, Drug-Offenders, (Forest-Offenders), Goondas, Immoral Traffic Offenders and Slum-Grabbers for Preventing their Dangerous Activities Prejudicial to the Maintenance of Public Order, Act

[71] AIR 2002 SC 3533.

(Tamil Nadu Act 14 of 1982), by an order of detention made by the Commissioner of Police, Madras, second respondent herein. The main ground of detentionare that the petitioner was indulging in offences under Section67 of the Information Technology Act, 2000, Sections 4 and 6 of the Indecent Representation of Women (Prohibition) Act, 1986 and under Section 27 of the Arms Act, 1959.The petition was failed and the same was dismissed.

In this case, *Fatima Riswana* v. *State Rep. by A.C.P., Chennai and Ors.*[72] Supreme court observed that The appellant is a prosecution witness in S.C. wherein respondents are the accused facing trial for offences punishable under Section 67 of Information Technology Act, 2000 read with Section 6 of Indecent Representation of Women (Prohibition) Act, 1986, Under Section 5 and 6 of Immoral Traffic (Prevention) Act, 1956, Under Section 27 of Arms Act, 1959 and Sections 120(B), 506(ii), 366, 306 and 376 I.P.C. The said trial relates to exploitation of certain men and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The said sessions trial came to be allotted to the Fast Track Court, Chennai which is presided over by a lady Judge. That court also happened to be the "Mahila Courts" constituted vide Government Notification G.O.Ms. No. 556 Home (Courts II) Department of the Tamil Nadu Government, constituted to exclusively deal with offences against women and for speedy trial of cases of offences committed against women and also case under other Social Laws enacted by the Central and the State Governments for the protection of women. In this case, Leave was granted.

In the *Bachpan Bachao Andolan* v.*Union of India (UOI) and Ors.*, [73]Supreme Court observed that Learned Solicitor General submitted that in the Ministry of Family Welfare and Child Development, a division needs to be created to deal with issues arising out of dissemination of publications which are harmful to young persons, publishing pornographic material in electronic form as well as the enforcement of Section 293 of the Penal Code. It is submitted that a further research study must be undertaken on the efficacy of the provisions of the Young Persons Harmful Publications Act, 1956, Section 67 of the Information Technology Act, 2000 and Section 293 of the Penal Code. It was held that No child shall be deprived of his

---

72 AIR 2005 SC 712.

73 AIR 2011 SC 3361.

fundamental rights guaranteed under Constitution of India and bring to child traffic and abuse.

4.3.3. 3. Cyberbullying

This is a very sensitive issue for many countries, since standards and definitions vary widely from place to place. Bullying is an attempt to raise oneself up by directly demeaning others. The attacker hopes to improve his social status or self esteem by putting others down. The term cyberbullying typically refers to online abuses. Discussions about cyberbullying generally revolve around children of school-going age and often call on schools to address the issue. The term bullying in the physical world tends to describe conduct that occurs when someone uses force or coercion to control another person. Such behaviour is seen to be habitual. It can involve tormenting, threatening, harassing, humiliating, embarrassing or otherwise targeting a victim.[74]

4.3.4. Computer Sabotage Offences

This type of cybercrime covers crime, which affects the security, integrity, confidentiality and reliability of information on computer systems. It includes all unauthorized access and unauthorized modifications.

4.3.4.1. Unauthorized Access to Computer Systems

Crimes surrounding unauthorized access to computer systems can be divided into two parts: unauthorized access per se and unauthorized access with the intention to commit another crime. In early 2009, some ghost hackers from China were revealed to have compromised 1,295 computers belonging to embassies, banks, news agencies across the world and The North Atlantic Treaty Organization (Information Warfare Monitor 2009 and Information Warfare Monitor and Shadow server Foundation 2010). They also managed to hack the computers used by the Tibetan government in exile at Dharamshala. This type of crime covers the famous 'hacking' and 'cracking' crimes where a person who is unauthorized to enter a particular computer system does so. It also covers the unauthorized interception of data.[75]

---

74 Anjali Kaushik, *Sailing Safe in Cyberspace* p.40 (SAGE Publication Ltd, London, 1st edn.,2013).

75 *Ibid.*

4.3.4.2. Unauthorized Modification

The crime of unauthorized modification is a serious one since it affects the integrity and availability of the computer system. It is exemplified clearly in most terrorist attempts to ruin the critical infrastructure of a particular nation. Viruses are also usual tools in this sort of crime. Modifications can be made by changing, adding or deleting data on the computer system. They can be either temporary or permanent. Singapore law provides for two years' imprisonment for this particular crime. [76]

4.4. Types of Cyber Crimes

There have been various kinds of computer and internet related crimes. The growth of crime on the internet is directly proportional to the growth of internet itself and so is the variety of crimes being committed or attempted. Some of these crimes are:

4.4.1. Computer Viruses

Viruses are computer programmes that migrate from computer to computer and attach to the computer operating system. Virus is a programme that infects a computer by inserting a copy of itself into the computer and damages the computer ill some manner, generally without the computer user's awareness.[77]Borrowed from the medical dictionary, the term describes the nature malignancy, which affects a computer system. It is defined as a living thing, too small to be seen without a microscope that causes infectious disease in people, animals and plants.[78]

The very definition explains as to why the term is used in cyber terminology. The word is further defined as instructions that are hidden within a computer program and are designed to cause faults or destroy data. The replicating characteristic calls for the use of the word "virus" which is the most appropriate term to address it. The short list for most dangerous viruses, which are to be guarded against to avoid mass destruction, includes Love Letter or ILOVEYOU, CIH or Chernobyl, Melissa, Magistr, Code Red, Nimda and Resume.[79]

---

76 *Ibid.*

77 Farooq Ahmad, *Cyber Law in India* p.318 (New Era Publication, Delhi, 4^{the} edn., 2013).

78 Sally Wehmeier (eds.), *Oxford Advanced Learner's Dictionary of Current English* (Oxford University Press, 7th edn., 2005).

79 Talat Fatima, *Cyber Crimes* pp.63-64 (East Book Company,1st edn.,2011).

In India, the Information Technology Act, 2000 defines "virus" in Section 43 in the following words:

> **Section 43, Explanation.**- "*For the purposes of this section,- (iii)'computer virus' means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource*".

The typical characteristic of a virus is that it attaches itself to the desired computer, remains dormant for a while and only infects the files, data that are run on the system. Viruses come in myriad forms like viruses, which aim at disabling a specific function or sleeping virus, or viruses, which have global effect like the "Love Bug" virus, which infected innumerable computers in 2000. The origin of computer viruses can be traced back to John von Neumann's studies of self-replicating mathematical automata in the 1940s. It was only in the 1970 that the idea of programs that could infect computers was initiated and the first well-documented case of a computer virus spreading in the wild occurred in October 1987, when a code snippet known as the Brain virus appeared on several dozen diskettes at the University of Delaware. The entire catena of viruses, which have the potentiality to contaminate computers, can be classified into three broad headings depending on the area or spot where they choose to reside and the kind of harm they thus cause:[80]

1. File infectors.

Usually hiding in spreadsheet programs or games, the virus remains unnoticed by the user until it executes. If a diskette/file is infected, it will infect another healthy computer.

2. Boot-sector viruses

Residing in the diskette or hard disk, it is read into the computer's memory and hence, the normal time of its execution is when the system is started/ restarted. It infects any diskette in the drive.

---

[80] *Id.* at p.160.

3. Macro viruses

Swift and independent of operating systems, the hideout of these viruses is data or files and they are usually in the form of scripts, which are used to automate actions.

4.4.2. Logic Bombs

Viruses, which may activate at a desired time or date are called time bomb and the viruses, which activate upon the happening of some event are called logic bombs. Logic bombs and time bombs are together called dropdead devices as they can be executed at the will of the person. It is a sort of code that is added to computer system and goes off at specific time, thus making system unusable. Specie of malicious code, which is conditional and dependent by nature, causes breach of security at the commanded time and on the occurrence of certain conditions. It is formally defined as: a code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security compromising activity whenever specified conditions are met.[81] This is a program which is used for targeting corporations, industries, etc. and to commit even a variety of traditional crimes like mischief, extortion and can act either instantly or at a future date. As it targets chosen, systems a chain of destructions is hardly perceived, thereby the loss is confined within certain limits.[82]

An examination of all the above programs reveals that viruses are the most damaging and fastest programs of all of these as they have the tendency to infect through the medium of files, disks, and hard disks attached to it. In the present cyber age, the transmission of information (files) is the sine qua non of the entire electronic activity, thereby making it vulnerable to external harming agents and thus, allowing the perpetrators to achieve their goals. Virus writing was in the beginning a pastime for the underground so much so that even virus-construction-kits appeared though they were not very helpful and effective for the layman. There are even instances of encrypted virus which made it difficult for the virus scanner to capture the virus's signature and identify it.[83] Because of this, Logic Bomb appears to be the least harming as it works within defined limits. Trojan horse is the most challenging one as

---

81 *See, available at: hattp//:*www.huis.hiroshimau.ac.jp/Computer/Jargon/Lexicon Entries/Logic_bomb. html. (last visited on May 10, 2012).

82 Talat Fatima, *Cyber Crimes* p.163 (East Book Company,1st edn.,2011).

83 Peter Stephenson, *Investigating Computer-Related Crime* p.6 (CRC Press, Washington 2000).

it implies deception, and its discovery and destruction are made evident simultaneously.

4.4.3. Trojan Horse

Trojan horse is apparently innocuous. It contains hidden functions. These functions are loaded onto the computer's hard drive and executed along with the regular programme. This innocuous programme carries inside its belly a sub-programme that performs a function that is generally known to its user. Love Bug of May 2000 is an example of Trojan Programme.

Trojan horse is a harmless and friendly-looking enemy which causes erosion and loss, when active. Its deceptive look is its primary connotation whereby it cannot be checked or controlled until the damage is done. It is used as a camouflage for the harmful and malignant designs of the perpetrator. Its surreptitious attack makes it difficult to intercept or control it at the right moment. It is designed as something as benign such as a directory lister, archiver, game or even a program to find and destroy viruses.[84] It is also used to capture the passwords of legitimate users of the system, which is done by impersonating the normal system logon program. A special case of Trojan horse is the Mockingbird Software that intercepts communications (especially login transactions) between users and hosts and provides system-like responses to the users while saving their responses (especially account IDs and passwords).[85]

4.4.4. Worms

Worms infect a computer system without being attached to its operating part. It moves from one computer to another computer. Worms has many things common with virus but is different from virus in many respects. Worms has the potential to grow exponentially and wind their way through the internet. They can cause extensive damage in overload servers and an anti-worm extraction.[86] Typical of the internet and network computers, this malicious program is yet another external agency, which has the characteristic feature of multiplying and spreading over the entire network. Their main dependency is on e-mail and internet relay chat through which they travel to

---

84 *See, available at: hattp//:*www.netmeg.net/jargon/terms/t.trojan_horse.html (last visited on May 18, 2013).

85 Talat Fatima, *op.cit.* p.162.

86 Farooq Ahmad, *Cyber Law in India* p.324 (New Era Publication, Delhi, 4^{the} edn., 2013).

unknown destinations. It is a program that propagates itself over a network, reproducing itself as it goes. Nowadays, the term has negative connotations, as it is assumed that only crackers write worms. A worm is a program that travels from one computer to another without attaching itself to the operating system of the computer. It infects unlike a virus, which attaches itself to a computer's operating system, and can later infect the operating system of any computer that uses a file taken from the infected computer.[87] Biggest challenge given by the menace of worm in the history of information technology is the internet Worm of 1988 released by a computer prodigy, Robert Tappan Morris who was later prosecuted or the crime and convicted.[88]

4.4.5. Computer Related Fraud

It is a form of white-collar crime whose growth may be as rapid and diverse as the growth of internet itself. According to the consumer organization Internet Fraud Watch (IFW), the number of consumer complaints it receives about internet fraud schemes has risen dramatically in the past two years, from 1152 in 1996 to more than, 7500 in 1998.[89]

4.4.6. Trapdoor

Trapdoor makes possible a person to have an access to the areas in the computer where permission is needed e.g. access only with the help of password. The access to a computer or information on computer may be possible only when a user has a password. A user can circumvent this requirement with the help of trapdoor. Trapdoor constitutes variety of programming methods that adversely affect the integrity of the computers.[90]

4.4.7 Bacterium

It affects processing and memory capacity of a computer system. It impairs efficiency of the computer unless computer makes full use of its potential to process

---

87 Jonathan Roosenoer, *Cyber Law* p.172 (R.R. Donnelley and Sons, Harrison Burg, New York 1997).

88 Talat Fatima, *op.cit.* pp.161-162.

89 See, *available at: hattp//:www.natlconsumersleague.org/top10net.html*(last visited on June 11, 2013).

90 Farooq Ahmad, *Cyber Law in India* p.324 (New Era Publication, Delhi, 4^{the} edn., 2013)

and memorize the information. Computer infected by the Bacterium cannot function efficiently.[91]

4.4.8 Salami Techniques

Salami techniques help in the commission of fraud in money transactions. Money is stolen in such small sums from a large number of users that it does not make a market difference overall. Salami techniques involve use of Trojan horse or secret execution of an unauthorized programme that enables stealing of insignificant amounts from large number of account holders.[92]

4.4.9. Denial of Service

Information Technology Act makes denying of or causing to deny access to any computer, computer system or computer network by any means, punishable if it is made without the permission of the owner or incharge of the computer, computer system or computer network.[93]

4.4.10. Smurf Attack

A hacker who tries to bring down a computer by smurf attack sends an echo request packet on 'ping' command to a computer network with the return address of the targeted victim. The victim's computer gets paralyzed if it is connected to a large network that will send large number of ping requests to overwhelm the computer.[94]

4.4.11. Internet Control Message Protocol (ICMP) Attack

Internet control message attack deals with error messages that the server sends to client in case former does not receive a response from the latter that the 'packet' has been received. It also handles 'pings' that are small 'feelers' working like an advance traffic control party.[95]

4.4.12. User Datagram Protocol (UDP) Attack

User datagram protocol provides information about the server's local time, echo, chargen etc. to other computers. Thus, User Datagram Protocol (UDP) 'time'

---

91 *Ibid.*
92 *Ibid.*
93 *Ibid.*
94 Farooq Ahmad, *Cyber Law in India* p.324 (New Era Publication, Delhi, 4^{the} edn., 2013).
95 *Ibid.*

protocol provides the time in a site independent, machine-readable format. When a server receives multiple User Datagram Protocol (UDP) requests, it becomes paralyzed because of its inability to respond to all these requests quickly. Thus, the server's processing capacity is exhausted by false requests.[96]

4.4.13. Multipronged Denial Service Attack

A hacker in this case, instead of using one computer to launch an attack uses many computers to target a compute from many fronts. The hacker uses a third party computer popularly called 'Zombies' or 'Soldiers' to launch adoemon or a small computer programme. The attacker uses many sources difficult for the target server to block off the attack routs.[97]

4.4.14 Password Sniffing

It pertains to use of a computer programme that monitors and records the names and passwords of network, users as they log in, thereby jeopardizing the security of the site.[98]

4.4.15 Spoofing

Spoofing is the act of electronically disguising one computer for gaining access to a restricted system.[99]

4.5. Cyber Crime and Information Technology Act, 2000

Cybercrime raised fears about the security of business process outsourcing operations in India, which has become one of the hubs for operations outsourced by countries like the United States, United Kingdome and other European countries. However, the Indian government, as well as the industry, has been taking proper care to handle these fears and to tighten security guidelines and frameworks to be followed by companies that handle outsourced operations. There have been continuous amendments in Indian cyber laws. In India cybercrime is dealt with by both the Indian Penal Code (hereinafter referred to as IPC) and the Information Technology Act, 2000, which was amended in 2008.[100]

---

96 *Ibid.*

97 Farooq Ahmad, *Cyber Law in India* p.324 (New Era Publication, Delhi, 4^{the} edn., 2013).

98 Indian Police Journal p.92 (April-June 2004).

99 *Ibid.*

100 Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.274 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn.,2000).

Since policing is a matter under the jurisdiction of the state, and complaints have to be lodged with the local police, most cybercrimes are registered under the IPC. The police at the local level therefore need to be conversant with the Information Technology Act or it will be difficult to prove cybercrimes. India also needs to build up its cyber forensic capabilities. [101] Information Technology Act, which was passed with the objective of promoting a secure electronic environment, deals with issues subsidiary to secure electronic environment such as contravention relating to electronic transaction and information technology offences. It also seeks to set up various authorities to help regulate an information technology regime.[102]

The Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) and Amendment in 2008 The Information Technology Act, 2000, a legal framework for transactions carried out electronically, was enacted to facilitate E-Commerce, e-governance and to deal with computer-related offences. Over the years, with several new forms of computer crime, misuse and fraud taking place, a need was felt to strengthen the legislation pertaining to information security. The government had enacted the IT Act, 2000 to focus on the evidential value of electronic transactions and provide legal recognition to electronic documents. Leveraging the experience gained, amendments to the IT Act, 2000 were approved by Parliament on 22th December 2008 to strengthen provisions in respect of data protection, e-governance, and technological utility in respect of signatures, new computer offences such as phishing, identity theft, e-commerce frauds, impersonation, video voyeurism and data retention. The amendments also provide for liabilities of service providers and intermediaries in the event of deficient services. The Information Technology (Amendment) Act, 2008, has been published in the Official Gazette. The amendment upgrades the existing legal framework to instil users' and investors' confidence in the area of information technology in the country. [103]

[101] Anjali Kaushik, *Sailing Safe in Cyberspace* p.198 (SAGE Publication Ltd, London,1st edn.,2013).

[102] Nadan Kamath, *Law Relating to Computers Internet and E-Commerce* p.274 (Universal Law Publishing Co.Pvt.Ltd, 2nd edn.,2000).

[103] Anjali Kaushik, *Sailing Safe in Cyberspace* p.198 (SAGE Publication Ltd, London,1st edn.,2013).

4.5.1. Penalties and Adjudication

Indian Parliament has adopted two-fold strategy to control cyber crimes. It has amended Indian Penal Code (IPC) to cover cyber crimes expressly and has provides provisions in the Information Technology Act, which was enacted to facilitate Electronic Commerce in India, to deal with compute related crimes. The Information Technology Act has extra-territorial jurisdiction and applies to any offence or contravention of the Information Technology Act. This feature of Information Technology Act is not unusual. Similar provision is found in the Information Technology legislations of other jurisdiction also.[104]

[104] See, Sec. 12 of The Information Technology Act,2000, Sec. 4 of The British Computer Misuse Act, 1993 As Amended 1998 and Sec. 9 of The Malaysian Computer Crime Act, 1997.

Schemes of the Act to curb computer crimes are as under:

Section	Offence	Punishment
65,43	Damage to computer, computer system etc	Compensation of Rs. 1 crore.
44(a)	Failing to furnish any document	Penalty not exceeding Rs 1 lakh 50 thousand rupees.
44(b)	Failing to file any return or furnishing information within the time prescribed.	Penalty not exceeding 5 thousand rupees for every day during which such failure continues.
44(c)	Not maintaining books of account or records.	Penalty not exceeding 10 thousand rupees for every day during which the failure continues.
45	Offences for which no penalty is separately provided.	Compensation not exceeding 25 thousand rupees
65	Tampering with Computer source document.	Imprisonment upto 5 years and fine upto Rs. 2 lakh rupees or both.
66	Hacking with computer system with the intend or knowledge to cause wrongful loss.	Imprisonment upto 3 years or fine which may extend upto 2 lakh rupees or both.
67	Publication of obscene material in an electronic form.	Imprisonment upto five years and fine upto Rs. 1 lakh and in the event of second or subsequent conviction, imprisonment upto 10 years and fine upto Rs. 2 lakhs or both.
68	Failing to comply with the directions of the controller.	Imprisonment upto 3 years and fine upto 2 lakh or both.
69	Failing to extend facilities to decrypt information which is against the interest of sovereignty or integrity of India.	Imprisonment upto 7 years.
70	Securing or attempting to secure access to a protected system.	Imprisonment which may extend to 10 years and fine.
71	Misrepresentation before controller or certifying authority for obtaining digital signature licence.	Imprisonment upto 2 years or fine up to Rs. 1 lakh or both.
72	Break of confidentiality and privacy.	Imprisonment upto to 2 years of fine upto Rs. 1 lakh or both.
73	Publishing digital signature certificate false in certain particulars.	-Do-
74	Publication of digital signature certificate for fraudulent purpose.	-Do-
76	Any computer, system, floppies, compact disks, tap drives or any other accessories related thereto used for contravention of this Act, rules, orders or regulations.	computer Liable to confiscation.

4.5.2. Miscellaneous Provisions

Chapter XIII of Information Technology Act, 2000 (hereinafter referred to as IT Act) contains sections 80 to 94. Section 80 provides that notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police Officer not below the rank of Deputy Superintendent of Police or any other of Central Government or State Government authorized by Central Government or State Government authorized by Central in the behalf, may, enter any public place and search and arrest without warrant any person found there in who is reasonably suspected to have committed any offence under this Act.

The term "public place" is defined to include any public conveyance any hotel, any shop or any other place intended for use by, or accessible to the public. As per this clause, no private complaint can be entertained by the officer in charge of a police station. Such complaint should be made to a Deputy Superintendent of Police. Section 87 confers power upon the Central Government to make rules by notification in the official gazette and in the electronic gazette. The required rules made by the Central Government should be published in the official gazette as well as in the electronic gazette (i.e. gazette published in the electronic form).Section 88 provides for constitution of Cyber Regulations Advisory Committee to advise the Central Government on certain matters under the Act. This Committee shall advice the controller in framing the regulation under the Act. Section 89 provides for power to the controller to make regulation under the Act. Section 90 empowers State Government to make rules to carry out provision of the Act.

4.5.3. Consequential Amendments to Existing Laws

The Act has consequential amendments to other laws to provide recognition for electronic documents and digital Signatures to facilitate the growth of E-Commerce as indicated below:

4. 5.3.1.Indian Penal Code

Section 91 provides for amendment of the Indian Panel Code. The Indian Panel Code provides for offences relating to documents such as forgery. It is proposed to amend seventeen sections so as to bring offences relating to electronic records also within the purview of Indian Penal Code. According to amendment few changes as follows:

(1) A new definition clause containing “electronic record' has been inserted as section 29A;[105]

(2) Sections 167,172, 173, 175, 192,204 and 463 of the IPC has been amended to include electronic record also as documents;

(3) Section 464 of the IPC is amended to provide punishment for making false electronic records;

(5) Sections 466,468,469,470,476 and 477A of the IPC are amended to include "forged electronic record” also within the scope of these sections.

4.6. Meaning and Concept of Jurisdiction

Jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property and subject matter. All sovereign independent States possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arising within these limits.[106]The dictionary meaning of jurisdiction is legal power or the authority. This means that the power to decide the dispute arising out of any relation. In law, the word jurisdiction has been taken from two Latin words, ‘*Juris*’ means ‘law’ and '*dicere*' meaning ‘to speak’. It refers to the practical authority granted to a formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and by implication, to administer justice within a defined area of responsibility. In common English language, Jurisdiction is the authority given to a legal body or to a political leader (Prime Minister, President, etc.) to deal with legal matters, and to pronounce or enforce legal matters.[107]

Jurisdiction is the authority by which courts take cognizance of and decide cases. The word 'jurisdiction' is of large and comprehensive import and embraces every kind of judicial action. Jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property and subject matter. These principles of jurisdiction are enshrined in the Constitution of a Country and part of its jurisdictional

---

105 Tabrez Ahamad, *op.cit.* p.142.

106 Vakul Sharma, *Information Technology Law and Practice* p.249 (Universal Law Publication Co., 1st edn., 2004).

107 Shaunakbali, “Analysis on The Concept of Jurisdiction”, *avalaible at hattp://*www. jurisonline .in (last visited on May 15, 2011).

sovereignty.[108] The internet impacts in major ways upon questions of jurisdiction. Jurisdiction to prescribe laws and adjudicate disputes historically has been based on territorial principles. Suppose, a country found a person within its territory, it exercised jurisdiction over that person. The internet greatly diminishes the significance of physical location of the parties, because transactions in cyberspace are not geographically based. Moreover, the internet alters the power balance between distributor and consumer, because it gives consumers instant access to enormous amounts of information and highly sophisticated analytical tools. This affects the basis on which courts have analyzed the ability of parties and particularly consumers to make enforceable choices of law.[109]

The effectiveness of a judicial system rests on bedrock of regulations and regulations which define every aspect of a system's functioning and principally, its jurisdiction. A court must have jurisdiction, venues[110], and appropriate service of process in order to hear a case and render an effective judgment. Jurisdiction is the power of a court to hear and determine a case. Without jurisdiction, a court's judgment is ineffective and impotent. Such jurisdiction is essentially of two types, namely subject matter jurisdiction[111] and personal jurisdiction[112] and these two must be conjunctively satisfied for a judgment to take effect. It is the presence of jurisdiction that ensures the power of enforcement to a court and in the absence of such power, the verdict of a court, is, to say the least, of little or no use. Moreover,

---

108 Apart from judicial activity, a State's administrative, executive and legislative activity is also part of its jurisdictional sovereignty. See, R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.822 (Kamal Law House, Kolkata, 1st edn., 2008).

109 Dennis T Rice, "Jurisdiction and E Commerce Disputes in United States and Europe" Presentation by Committee on Cyberspace Law and Business Law Section at the Annual Meeting of the California State Bar, Monterey (October 12, 2002).

110 See, Black's Law Dictionary p.653 (pocket edn., 1996) defining venue as the possible or proper place or places for the trial of a suit, as among several places where jurisdiction could be established: Venue establishes the location where the power of a court should be exercised. It is decided on the basis of convenience and thus may be waived by the parties.

111 Subject matter jurisdiction is defined as the competence of the court to hear and determine a particular category of cases. It requires a determination of whether a claim is actionable in the court where the case is filed.

112 Similarly, personal jurisdiction is simply the competence of the court to determine a case against a particular category of persons. It requires a determination of whether the person is subject to the court in which the case is filed.

only generally accepted principles of jurisdiction would ensure that courts abroad also enforce the orders of other judicial bodies.[113]

Jurisdiction, of course, defines three kinds of power:

- The power to prescribe,
- The power to adjudicate, and
- The power to enforce.

The first of these relates principally to the power of a government to establish and prescribe criminal and regulatory sanctions. The second, to the power of the courts to hear disputes, especially civil disputes; and the third, to the power of a government to compel compliance or to punish non-compliance with its laws, regulations, orders, and judgments. internet jurisdiction can also be conceptualized in three layers. There is an application layer that determines whether courts are entitled to apply their laws to a particular dispute. Above the application layer is a substantive layer, where courts apply their substantive laws to the dispute above the substantive layer is the enforcement layer, where court orders must be enforced in an online environment that often resists the imposition of foreign judgments because of large distances and minimal monetary disputes. Jurisdiction is a word capable of many interpretations. A state's jurisdiction refers to the competence of the state to govern persons and property by its municipal law. In order for a national court to adjudicate criminal and regulatory sanctions internationally, there must be some connection, or nexus, between the regulating nation (the forum) and the crime or criminal. This is true whether the regulated conduct takes place in the physical world or in cyberspace.[114]

4.7. Various Principles of Jurisdiction under International Law

International law limits a country's authority to exercise jurisdiction in cases that involve interests or activities of no-residents. First, there must exist 'jurisdiction to prescribe'. If jurisdiction to prescribe exists, 'jurisdiction to adjudicate' and, 'jurisdiction to enforce' will be examined. Jurisdiction to prescribe means that the

---

113 Nandan Kamath, *Law Relating to computers, internet and E-commerce* p.22 (universal law Publishing Co. Pvt.Ltd, 2nd edn., 2000).

114 Tushar Kumar Biswas, "Data and Information Theft in E-Commerce, Jurisdictional Challenges, Related Issues and Response of Indian Laws" 27 *Computer Law and Security Review* pp.385-393 (2011).

substantive laws of the countries are applicable to the particular persons and circumstances. When a country has jurisdiction to prescribe, it can appropriately apply its legal norms to conduct.

Simply stated, a country has jurisdiction to prescribe law with respect to:

(1) conduct that, wholly or in substantial part, takes place within its territory,

(2) the status of persons, or interests in things, present within its territory,

(3) conduct outside its territory that has or is intended to have substantial effect within its territory,

(4) the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(5) certain conduct outside its territory by persons who are not its nationals that is directed against the security of the country or against a limited class of other national interest.

Jurisdiction to adjudicate means that the tribunals of a given country may resolve a dispute in respect to a person or thing where the country has jurisdiction to prescribe the law that is sought to be enforced. The exercise of jurisdiction by a country is subject also to the requirement of the reasonability.[115]

Traditionally, three kinds of jurisdiction are distinguished: jurisdiction to prescribe, or legislative jurisdiction, jurisdiction to adjudicate, or judicial jurisdiction, and jurisdiction to enforce, or executive jurisdiction. Jurisdiction to prescribe is the first step in many analyses. Jurisdiction to adjudicate does not apply in the absence of jurisdiction to prescribe unless the Forum State is willing to apply the law of a foreign State. For jurisdiction to enforce, States also regularly need jurisdiction to prescribe. These distinctions can be important in determining the limits of a country's jurisdiction under international law. Depending on the nature of the jurisdiction being exercised, the requisite contacts with a State necessary to support the exercise of jurisdiction differ. The three types of jurisdiction however, are often interdependent, and their scope and limitations are shaped by similar considerations.[116]

---

115 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.826 (Kamal Law House, Kolkata, 1st edn., 2008).

116 *Id.* at p.828.

4.7.1. Prescriptive Jurisdiction

'Jurisdiction to prescribe' means a State's authority to make its substantive laws applicable to particular persons and circumstances. International law has long recognized limitations on the authority of States to exercise jurisdiction to prescribe in circumstances affecting the interests of other States. In principle, it was accepted that a State had legislative jurisdiction to regulate activities within its territory, as well as the conduct of its nationals abroad. Yet, there is wide international consensus that not even the links of territoriality or nationality suffice in all instances for the exercise of jurisdiction to prescribe. For instance, according to Article 34 of the Vienna Convention on Diplomatic Relations 1961, diplomats are exempted from most dues and taxes.[117]

When the prescriptions of two States are in conflict, each State has an obligation to evaluate its own as well as the other State's interest in exercising jurisdiction. A State should defer to the other State if that State's interest is clearly greater. A State has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism.[118]

These principles are known as the territoriality principle, the nationality principle, the effects principle and the protective principle.

4.7.1.1. Territoriality Principle

The territoriality nexus holds that the place where an offence is committed-in whole or in part-determines jurisdiction. This is a favored basis for the exercise of state jurisdiction. Events occurring within a state's territorial boundaries and persons within that territory, albeit their presence temporary, are as a rule subject to the application of local law. So, if any act of information/data theft is committed in India the offender can be very well punished and prosecuted in India.[119]The territoriality principle is by far the most common basis for the exercise of jurisdiction to prescribe,

---

117 *Id.* at p.829.

118 *Ibid.*

119 Tushar Kumar Biswas, "Data and Information Theft in E-Commerce, Jurisdictional Challenges, Related Issues and Response of Indian Laws" 27 Computer Law and Security Review pp.385-393 (2011).

and it has been generally free from controversy. This principle would allow a State to order service providers who operate on its territory to obey its regulations. It would further allow barring access to certain Web sites from machines operating within the State's territory. States insist, in fact, on their sovereignty to control activities which happen in their territory even if these activities are not limited to the national territory and even if control might be ineffective.

The territorial principle has two variants:

(i) 'objective' territorial principle, where a State exercises its jurisdiction over all activities that are completed within its territory, even though some element constituting the crime or civil wrong took place elsewhere; and

(ii) 'subjective' territorial principle, where a State asserts its jurisdiction over matters commencing in its territory, even though the final event may have occurred elsewhere. [120]

In *SS Lotus Case (France* v. *Turkey)*[121] , it was held by the Permanent Court of a International Justice that the first and foremost restriction imposed by international law upon a State is that failing the existence of a permissive rule to the contrary . It may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial and it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".[122] The chances are that in view of components of acts involving territories of two or more States, the only way out to resolve the issue is through mutual negotiation, extradition to the most affected State (if extradition treaty exists between them) or simply by an exercise of jurisdiction by the State having custody of the accused.

4.7.1.2. Nationality Principle

The nationality nexus looks to the nationality or national character of the person committing the offence to establish jurisdiction. That means jurisdiction exercised on this principle relates to the nationality of the offender. The fact that jurisdiction may be claimed on the nationality principle does not preclude the state

120 *Ibid.*
121 PCIJ Ser A (1927), No. 9.
122 *Ibid.*

which the offence was committed for exercising jurisdiction on the territorial principle. That means if the offence of information/data theft is committed in any other countries other than India and the offender is an Indian citizen then the both Indian court as well as the court abroad will have jurisdiction to try the matter.[123]

The right of a State to regulate the conduct of its citizens or nationals anywhere in the world is, like territorial jurisdiction, basically noncontroversial. For example, more and more States are outlawing child sex tourism. This makes sexual intercourse with a child punishable for the adult even if the act is tolerated or legal in the country where the act is committed. In so far as Germany makes even its nationals residing abroad subject to its prohibition against the dissemination of child pornography. It is acting in accordance with international law. The nationality principle is applicable to juristic as well as to natural persons. As the German branch of CompuServe Inc., for example, is chartered as a German company, it is subject to German law. In addition to the territoriality principle, therefore, service providers will in many cases also be subject to jurisdiction under the nationality principle.[124] It is for each State to determine under its own law who are its nationals. Any question as to whether a person possesses the nationality of a particular State shall be determined in accordance with the law of that State. Nationality serves above all to determine that the person, upon whom it is conferred, enjoys the rights and is bound by the obligations, which the law of the State in question grants to or imposes upon its nationals.[125] Under the garb of nationality principle, a State may exercise jurisdiction over its own nationals irrespective of the place where the relevant acts occurred. A State may even assume extra-territoriality jurisdiction.

4.7.1.3. The Effects Principle

The effects principle can be invoked when an act committed in one State causes injury in the territory of another State. Jurisdiction is grounded in the fact that the injurious effect, although not the act or omission itself, occurred in the territory of the State. Controversies may particularly arise where the conduct was lawful where

---

123 Tushar Kumar Biswas, "Data and Information Theft in E-Commerce, Jurisdictional Challenges, Related Issues and Response of Indian Laws" 27 *Computer Law and Security Review* pp.385-393 (2011).

124 R.K.Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.831 (Kamal Law House, Kolkata, 1st edn., 2008).

125 Vakul Sharma, *Information Technology Law and Practice* p.251 (Universal Law Publication Co., 1st edn.,2004).

carried out. This principle has been a major source of controversy in anti-trust cases where it was invoked to support regulation of activities abroad by foreign nationals because of the economic impact of those activities in the regulating State. As a basis for jurisdiction however, it is increasingly accepted even when its excessive application, especially by the United States, is criticized.[126] It is an extra-territorial application of national laws where an action by a person with no territorial or national connection with a State has an effect on that State. The situation is compounded if the act is legal in the place where it was performed. The 'effects doctrine' is primarily a doctrine to protect American business interests and is applicable where there are restrictive trades or anti-competitive agreements between corporations. In *Hartford Fire Insurance Co.* v. *California*[127] the question was whether the London insurance companies refusing to grant reinsurance to certain US businesses, except on terms agreed amongst themselves are violative of the US anti-trust laws and tried in the United States. The US Supreme Court held that the US court did have jurisdiction and that there exists no conflict between domestic and foreign law and where a person subject to regulation by two States can comply with the laws of both.[128]

4.7.1.4. Protective Principle

The protective principle, found in Restatement Section 402(3), allows a State to protect its own governmental functions. International law recognizes the right of a State to punish a limited class of offences committed outside its territory by persons who are not its nationals. Nearly all States assume jurisdiction over aliens for acts done abroad which affect the security of the State.[129] These offences must be generally recognized as criminal by the international community. This is the case for offences like espionage, counterfeiting of the State's seal or currency, or falsification of official documents. Furthermore, hackers who play war games and intrude in national security data systems, or endanger the systems with worms[130] or through other means, face subjection to the jurisdiction of the affected State. The protective principle does not support application to foreign nationals of laws against political

126 R.K.Chaubey, *op.cit.* p.831.
127 113 S. Ct 2891 (1993).
128 Vakul Sharma, *op.cit.* p.253.
129 R.K.Chaubey, *op.cit.* p.832.
130 Marriam, *Webster's Collegiate Dictionary* p.1364 (10th edn., 1996). A worm is a usually small self –contained computer program that invades computers on a network and usually performs a malicious action.

expression. Considerations of national security, however, helped the House of Lords, in *Joyce* v. *Director of Public Prosecutions*[131] to decide that an alien who left the country in possession of a British passport owed allegiance and was guilty of treason when he subsequently broadcast propaganda for an enemy in wartime.

4.7.1.5. Universality Principle

Universality provides for jurisdiction over a crime which customary or conventional law labels as egregious as to be of universal concern. Unlike the other principles of jurisdiction, universality does not require a direct connection such as the place of the offence, the nationality of the offender, or the effects of the offence on the prescribing State. The required connection is more abstract. Universal jurisdiction over the specified offences is a result of universal condemnation of those activities. They are subject to universal jurisdiction as a matter of customary law or as a matter of international agreements. In the latter case, it remains to be determined whether universal jurisdiction over a particular offence has become customary law for States not party to such an agreement. The doctrine was developed centuries ago to address the piracy that menaced international trade and justified its application by deeming the pirate *hostes humani generi*-the enemy of all humankind. Meanwhile, Section 404 of the Restatement correctly reflects the consensus of the international community." It criminalizes piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and certain acts of terrorism. One might wonder whether any of these crimes might be committed in cyberspace but whoever cruises the Net for a while will not have many difficulties discovering Web sites, which at least give rise to a statutory interpretation of direct and public incitement to commit genocide. Especially in regions where war is being waged, it should also be possible to prove that people are serious about hate messages that are they really want genocide to happen. [132]

The canvass of the universality principle is quite vast. A State has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern. It includes acts of terrorism, attacks on or hijacking of aircraft, genocide, war crimes etc. A State may assert its universal jurisdiction irrespective of who committed the act and where it occurred. The perspective is broader as it was deemed necessary to uphold international legal order

131 1946 App Cas. 347.
132 R.K.Chaubey, *op.cit.* p.833.

by enabling any State to exercise jurisdiction in respect of offences, which are destructive of that order. The principles of jurisdiction of international law take cognizance of both State and international laws. If on one hand the objective of the State (or municipal or domestic) law is not only to ascertain the supremacy of its judicial sovereignty domestically but also extra-territorially, then on the other, the international law itself imposes general prohibition against the extra-territorial application of domestic laws.[133]

4.7.2. Jurisdiction to Adjudicate

Jurisdiction to adjudicate is defined as a State's authority to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the State is a party to the proceedings. It requires a sufficient or reasonable relation with the Forum State. A State may exercise jurisdiction through its courts to adjudicate with respect to a person or thing if the relationship of the State to the person or thing is such as to make the exercise of jurisdiction reasonable.[134] The fact that an exercise of jurisdiction to adjudicate is reasonable does not mean that the Forum State has jurisdiction to prescribe in respect to the subject matter of the action. Conversely, there may be circumstances in which a State has jurisdiction to prescribe but jurisdiction to adjudicate is absent or doubtful. Especially in criminal cases, jurisdiction to adjudicate is rarely exercised in the absence of jurisdiction to prescribe by the same State, because courts rarely apply the criminal laws of other States. In international criminal cases, jurisdiction to adjudicate depends almost exclusively on presence of the accused. In international civil cases, the principle of *actor sequitur forum rei* (Plaintiff follows defendant to the latter's forum) can be regarded as a principle accepted virtually everywhere.

It is important to note that the international law standard for civil cases reasonableness differs significantly from the U.S. Minimum contacts standard which was crafted in *International Shoe* v. *Washington and serves*[135] as the basis for deciding jurisdictional questions in the U.S. Transitory presence, for example, is not a sufficient basis for the exercise of jurisdiction to adjudicate under international law even though tag jurisdiction is in accordance with U.S. law. One federal court even

---

133 Vakul Sharma, *op.cit.* p.253.
134 R.K.Chaubey, *op.cit.* p.835.
135 326 U.S. 310, 316 (1945).

held that the temporary presence of a person within the airspace of a state while on board a commercial aircraft established jurisdiction. As a matter of principle, international law requires closer pre-litigation contacts between the defendant and the Forum State than would be necessary in domestic cases. This is due to the fact that a foreign nation presents a higher sovereignty barrier than another State within the United States. U.S. courts generally agree upon this concern for other nations' sovereignty. Internet-related questions involving jurisdiction have been most common in U.S. courts, primarily because of the multi jurisdictional character of the country. U.S. courts have taken various approaches to this jurisdictional issue. It is helpful to separate these approaches into two categories: moderate and expansive. The moderate approach is more consistent with the reasonableness standard of international law and is a better model for international multi-jurisdictional cases.[136]

4.7.2.1. Moderate perspective

Nine domestic courts so far have taken a moderate approach that is consistent with an international reasonableness standard. One court refused to find jurisdiction based solely on the existence of a Web site where it was not established that the Web site was accessed by citizens of the Forum State. Another court refused to find jurisdiction where the contents of a Web site were unrelated to the cause of action. In the other cases, the accessibility of a Web site within the state was not an adequate basis for jurisdiction. In two out of these seven cases, jurisdiction based solely on internet advertising was denied. In four cases, more than internet advertising was involved. The courts upheld jurisdiction because of numerous intentional contacts to the Forum State. In a final case, jurisdiction was denied where the only contact with the Forum State was the location of a database.[137]

4.7.2.2. Expansive perspective

A hint of international jurisdictional issues central to this analysis was present in *State* v. *Granite Gate Resorts, Inc.,*[138] Granite Gate Resorts was litigated too soon for international issues to arise; the defendants were preparing to operate their computer service from Belize, but they had not yet done so at the time of suit. Although such issues were not directly resolved, this court and others have expanded

136 *Ibid.*
137 *Ibid.*
138 (1997) 568 N.W. 2d 715.

their jurisdictional reach into cyberspace. The cases demonstrate approaches that move toward a rule calling for jurisdiction over a defendant in all States based on the accessibility of the defendant's Web site by users in all States. If this rule was adopted internationally, a defendant would be subject to the jurisdiction and differing laws of every State worldwide.[139]

4.7.3. Enforcement Jurisdiction

Jurisdiction to enforce deals with a State's authority to induce or compel compliance or to punish noncompliance with its laws or regulations whether through the courts or by use of executive, administrative, police, or other non judicial action. The U.S. enforcement agencies, in particular, are starting to enforce national laws on the internet. It is widely assumed that a State may not enforce its rules unless it has jurisdiction to prescribe those rules. The mere existence of jurisdiction to prescribe, however, is insufficient to justify the state to exercise enforcement jurisdiction in another state's territory. Especially concerning measures in aid of enforcement of criminal law, a State's law enforcement officers may exercise their functions in the territory of another state only with the consent of the state, given by duly authorized officials of that state.[140]

Enforcement measures requiring consent include not only the physical arrest of a person, but also, for example, service of subpoena, orders for production of documents, and police inquiries. Police investigations may, therefore, not be mounted on the territory of another State without its consent. The consequences may seem odd for anyone not familiar with the eagerness of States to protect their national sovereignty. Enforcement jurisdiction is linked quite closely to the territory. Its limits are much more strictly observed than is the case with jurisdiction to prescribe. An interesting question arises when the investigation is accomplished without entering another State's territory, by running, for instance, a computer program that searches databases installed in another country. At least two different scenarios are imaginable. Police could send dog sniffs via network to hard drives to check their contents. Law enforcement agencies could try to filter the streams of e-mail communication by searching for certain keywords, evaluating the communication in certain news groups, or checking suspicious Web sites. The first scenario is

---

139 *Id.* at p.837.
140 *Id.* at p.838.

distinguished from the second insofar as the objects of supervision, hard drives, have a certain territorial location. Even though they can be easily moved, they are like all tangibles always physically located, either within or outside the borders of a certain jurisdiction. It is much more difficult to locate Web sites or public bulletin boards. Even when the location of a hard drive, a Web site, or a bulletin board is known, the question is whether the activity of a foreign law enforcement agency might be allowed because the territory was not physically entered by any agent.[141]

4.8. Internet Jurisdiction

The first use of the term cyberspace was in 1984 by author William Gibson in his science fiction novel *Neuromancer*. It described the virtual world of computers. Today, cyberspace is how most people describe the world of the internet. Cyberspace is a 'borderless' world. It has no geographical boundaries and it establishes immediate long-distance communications with anyone who can have access to any website. Usually an internet user has no way of knowing exactly where the information on a site is being accessed. In cyberspace, jurisdiction issues are of primary importance. As, internet does not tend to make geographical and jurisdictional boundaries clear, internet users remain in physical jurisdictions and are subject to laws independent of their presence on the internet, Therefore, any kind of use of the World Wide Web and any related activities on the internet may expose the person to risk of being sued in any state or foreign country where another internet user may establish a claim. Accordingly, in each case, a determination should be made as to where an online presence will subject the user to jurisdiction in a distant state or a foreign company. The whole trouble with internet jurisdiction is the presence of multiple parties in various parts of the world who have only a virtual nexus with each other. Then, if one party wants to sue the other, where can he sue? Traditional requirements generally encompass two areas - firstly, the place where the defendant resides, or secondly, where the cause of action arises.[142]

However, in the context of the internet, both these are difficult to establish with any certainty. Even a childishly simple' transaction can give rise to a mind-boggling issue of jurisdiction on the Net. For example, A, in India, decides to

---

141 *Ibid.*

142 Nandan Kamath, *The Law Relating to Computers, Internet and E-Commerce* p.25 (Universal Law Publication Co.,2nd edn., 2000).

download an article from a website, pays money for it through a credit card, and then is unable to perform the download. He wants to sue the owner of the site. But the owner is in Thailand. The site itself is based in a server in Brazil. Where does the defendant reside? The transaction occurred on the net. So was it in India, or in Brazil?[143]

Internet jurisdiction can also be conceptualized in three layers. There is an application layer that determines whether courts are entitled to apply their laws to a particular dispute. Above the application layer is a substantive layer, where courts apply their substantive laws to the dispute. Above the substantive layer is the enforcement layer, where court orders must be enforced in an online environment that often resists the imposition of foreign judgments because of large distances and minimal monetary disputes.[144]

As such, a single transaction may involve the laws of at least three jurisdictions:

(1) The laws of the state/nation in which the user resides,

(2) The laws of the state/nation that apply where the server hosting the transaction is located, and

(3) The laws of the state/nation which apply to the person or business with whom the transaction takes place.

It is worth examining the decision in *Cybersell, Inc.* v. *Cybersell, Inc*[145] as a typical example of a fact situation involving a conflict over jurisdiction. The case involved a service mark dispute between two corporations, one at Orlando and another at Arizona. The court had to address the issue of whether the mere use of a web site by the Florida Corporation was sufficient to grant the Court, in Orlando, jurisdiction. The Court answered the question in the negative, focussing on traditional analysis established by the US Supreme Court concerning the due process aspects of personal jurisdiction: it is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the

---

143 Nandan Kamath, *The Law Relating to Computers, Internet and E-Commerce* p.25 (Universal Law Publication Co.,2nd edn., 2000).

144 Tushar Kumar Biswas, "Data and Information Theft in E-Commerce, Jurisdictional Challenges, Related Issues and Response of Indian Laws"27 *Computer Law and Security Review* pp.385-393 (2011).

145 1997U.S. App. LEXIS 33871 (9th Cir., December 2,1997).

forum State, thus invoking the benefits and protections of its laws. The court rejected the plaintiff's argument that by employing a web page, without more a web publisher was subject to jurisdiction in the plaintiff's forum. The Court also rejected the plaintiff's reliance on the effects test, holding that the test does not apply with the same force to a corporation as it does to an individual "because a corporation does not suffer harm in a particular geographic location in the same sense that an individual does.

A similar result was reached in *Smith* v. *Hobby Lobby Stores Inc. v. Boto Co. Ltd.*[146] The court held there were insufficient contacts for personal jurisdiction over the counter-defendant, where this company had no real contact with the state aside from a Web page that could be accessed from the state. However, decisions of this nature do not solve the entire issue. Not only are there contradictory judgements, but more complex fact situations give rise to progressively confusing holdings, with little or no consistency.

For example, in *Edias Software International, L.L.C.* v. *Basis International Ltd*[147], the contractual relationship between an Arizona limited liability company and a New Mexico corporation combined with the defendant's use of the internet was used to justify jurisdiction in Arizona notwithstanding that the contract provided that it would be governed by the law of the State of New Mexico.

Another illustrative matter is that of *United States* v. *Thomas*[148], which involved a California couple who operated a computer bulletin board. That contained various sexually explicit images, and offered sexually explicit videotapes for sale. A United States postal inspector, surfing the web, came across the web site and applied for membership on the bulletin board from his office in Tennessee. He also ordered several videotapes. After the password was issued and the tapes delivered, the couple was arrested. They were indicted in the Western District of Tennessee and charged with various violations of federal obscenity laws. Obscene was required to be judged, inter alia, by contemporary community standards. The prosecution argued that the court should apply the community standards of Memphis, Tennessee, where the allegedly obscene materials were received. The defence, on the other hand, argued

146 968 F. Supp. 1356 (W.D. Ark. 1997).
147 947 F.Supp. 413 (D.Ariz. 1996).
148 74 F.3d 701 (6th Cir. 1996), cert. denied, _ U.S. --,117 S. Ct. 74 (1996).

that the defendants should be judged by the community standards of Milpitas, California, or, failing that, by the standards of cyberspace itself.

While dismissing this argument, the court noted that the defendants were technologically able, if they had so chosen, to limit user access in jurisdictions with more restrictive obscenity laws than those in California. Because defendants knew they had a member in Memphis, they could be held to the moral standards of that community. Thus, because the defendants entered into a transaction with a member in Memphis, they could be judged by reference to those standards.[149]

4.8.1. Convention on Cyber Crime

The 'Convention on Cyber crime' was opened at Budapest on 23rd November 2001 for signatures. It was the first ever-international treaty on criminal offences committed against or with the help of computer networks such as the internet. The Convention deals in particular with offences related to infringement of copyright, computer-related fraud, child pornography and offences connected with network security. It also covers a series of procedural powers such as searches of an interception of material on computer networks. Its main aim, as set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cyber crime, inter alia, by adopting appropriate legislation and fostering international co-operation.[150]

4.8.2. Extraditable Offences

Extradition procedures are designed not only to ensure that criminals are returned from one country to another but also to protect the rights of those who are accused of crimes by the requesting country. Thus, sufficient evidence has to be produced to show a prima facie case against the accused and the rule of speciality protects the accused from being tried for any crime other than that for which he was extradited.[151]

---

149 Nandan Kamath, *The Law Relating to Computers, Internet and E-Commerce* p.28 (Universal Law Publication Co.,2nd edn., 2000).

150 Vakul Sharma, *Information Technology Law and Practice* p.256 (Universal Law Publication Co., 1st edn., 2004).

151 *Ibid.*

Similar views were expressed by the Supreme Court in *Daya Singh Lahoria* v. *Union of India,*[152] A fugitive brought into this country under an extradition Decree can be tried only for the offences mentioned in the extradition decree and for no other offences and the criminal courts of India will have no jurisdiction to try such fugitive for any other offence. There is no rule of international law which imposes any duty on a State to surrender a fugitive in the absence of extradition treaty. The law of extradition, therefore, is a dual law. It is ostensibly a municipal law; yet it is a part of international law also, inasmuch as it governs the relations between two sovereign States over the question of whether or not a given person should be handed over by one sovereign State to another sovereign State. This question is '(decided by national courts but on the basis of international commitments as well as the rules of international law relating to the subject.[153] It is significant to note that despite the treaty, a State may refuse extradition. In *Hans Muller of Nuremberg* v. *Superintendent Presidency jail, Cal*[154], the court held that even if there is a requisition and a good cause for extradition, the government is not bound to accede to the request, because S. 3(1) of the Indian Extradition Act, 1903 (based on Fugitive Offenders Act, 1881 of the British Parliament) gives the government discretionary powers.

Extradition is usually granted for an extraditable offence regardless of where the act or acts constituting the offence were committed. It is not granted for a political offence; the following shall not be considered to be political offences (and hence are extraditable offences) Murder or other wilful crime against a Head of State or Head of Government or a member of their family, aircraft hijacking offences, aviation sabotage, crimes against internationally protected persons including diplomats, hostage taking, offences related to illegal drugs, or any other offences for which both contracting slates have the obligation to extradite the person pursuant to a multilateral international agreement.[155]

---

152 (2001) 4 SCC 516.

153 Vakul Sharma, *Information Technology Law and Practice* p.256 (Universal Law Publication Co., 1st edn., 2004).

154 AIR 1955 SC 367.

155 Vakul Sharma, *Information Technology Law and Practice* p.256 (Universal Law Publication Co. 1st edn., 2004).

4.9. Personal Jurisdiction in Cyber Space

Unfortunately, very few cases concerning personal jurisdiction in cyberspace have been decided by the superior courts in India. For the purpose of determining, whether the cause of action arose in the local limits of a court, the courts generally go into the question of place of conclusion of the contract. However, it seems that the place of conclusion of contract would not be of much assistance in case of an E-Contract. There would be an insoluble confusion between the rules governing completion of communication of offer, acceptance and revocation.

The rule in *Bhagwandass Goverdhandas Kedia* v. *Girdharilal Purushottam & Co.*[156] would neither apply nor lend much support in reaching a reasonable solution in contracts entered into through the internet. Indian court would not decline jurisdiction merely on the ground that the international contract in entered through the internet. It examines the two bases of jurisdiction; domicile of the defendant and proximity to cause of action. Even if one were found to be satisfied, the Indian court it seems would assume jurisdiction. E-Commerce is 24/7 commerce. It is an online activity involving exchange of goods and services for a consideration (money). Such activity may lead to disputes, which could be (a) municipal (domestic) or (b) international. The question is how to resolve these disputes keeping in view the complexity of online activity. [157] The traditional principles of domestic and international jurisdiction that have been developed and adopted over a period of time are now being extended to cyberspace to formulate a new idiom of cyber jurisdiction. This adoption, in a way, would maintain continuity of established law and practice even in the realm of online activities.[158]

4.9.1. Personal Jurisdiction in Cyber Space: United State perspective

United States (hereinafter referred to as US) has developed their own respective long-arm statute to exercise jurisdiction over any matter. This jurisdiction may be divided into two parts:

---

156 AIR 1966 SC 543. The test laid down in this case is that in cases is of means of instantaneous communication, the contract is said to be concluded at the place where the acceptance comes to the knowledge of the proposer.

157 Vakul Sharma, *Information Technology Law and Practice* p.259 (Universal Law Publication Co., 1st edn., 2004).

158 *Ibid.*

(a) General jurisdiction, and

(b) Specific jurisdiction.

General jurisdiction subjects a person to the power of the applicable court with respect to any cause of action that might be brought. While specific jurisdiction refers to the power of the applicable court with respect to a particular cause of action based upon some set of minimum contacts with the forum state that relate to that cause of action. [159]

The principle of 'long-arm statute' authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action falls within the nature activity required to qualify for jurisdiction. The credit to establish ground rules for establishing personal jurisdiction lies with the US Supreme Court judgment in *International Shoe Co.* v. *State of Washington.*[160] It was held in this case that a court's exercise of personal jurisdiction over a non-resident defendant is proper if that defendant has had certain minimum contracts with the forum state such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice. This case also established criteria for minimum contacts.

Due to the amount of use of the internet and the traffic through Cyberspace in the U.S., there are many precedent cases that could help decide on the future legislation and jurisdiction of Cyberspace. Many cases in the United States have been examples because they demonstrate the use of the long arm of the law, and extending the jurisdiction of a State over a person in another. This personal jurisdiction is determined if a person has sufficient minimum contact. This minimum contact consists of physical presence, financial gain, stream of commerce, and election of the appropriate court via contract, with other jurisdiction. Long arm statutes have been used for many years now and have been seen in both good and bad light. Many nation States feel that within the U.S., the long arm statues are ok, however once the statutes leave the national boundaries, the affected States tend to believe that the U.S. is overstepping its bounds. The United States has to date, used standing laws and interpretations in order to provide itself with the jurisdiction that it needs to uphold law in Cyberspace.

---

159 *Id.* at p.260.

160 326 US 310 ,316 (1945).

In the case of *State of Minnesota* v. *Granite Gate Resorts, Inc.*[161] The United States extended its arm to affect an online betting company in Belize. This case shows how the United States allows not only the Jurisdiction in Cyberspace to be obtained by any State affected, it shows how they are capable of obtaining Jurisdiction over other nation States as well when it comes to international business.

It is important to understand the traditional principles of jurisdiction, like personal jurisdiction, local state's long-arm statute and the due process clause of the US Constitution to know how these principles have been used by various courts to resolve E-Commerce related disputes.

4.9.1.1. Personal Jurisdiction

Personal jurisdiction is the competence of a court to determine a case against a particular category of persons (natural as well as juridical). It requires a determination of whether or not the person is subject to the court in which the case is filed. [162] Personal jurisdiction looks into an issue from the point of 'physical presence', whether the person was a resident or a non-resident. If he is a resident, then there is no doubt about his being subject to municipal (domestic) laws. The problem arises, if he is a non-resident, what laws would be applicable - municipal laws of the state where he is residing or municipal laws of the state whose laws he has transgressed. It may be further classified into (a) "general" jurisdiction and (b) "specific" jurisdiction. [163]

4.9.1.1.1. General Jurisdiction

The "general" jurisdiction subjects a person to the power of the applicable court with respect to any cause of action that might be brought. It has historically relied on very close contacts of the person with the state, such as residency or domicile within the state, physical presence in the state at the time of service of process, or some other substantial "continuous and systematic" contact with the forum state.

---

161 See, in the case, *State of Minnesota* v. *Granite Gate Resorts. Inc.* Court File No. C6-95-7227. State or Minnesota District Court County Of Ramsey, Second Judicial District, *available at http:*//www.loundy.comlCASESlMinn_v_Granite_Gate.html. (last visited on June 1, 2013).

162 Vakul Sharma, *Information Technology Law and Practice* p.260 (Universal Law Publication Co., 1st edn.,2004).

163 *Ibid.*

4.9.1.1.2. Specific Jurisdiction

The "specific" jurisdiction, refers to the power of the applicable court with respect to a particular cause of action based upon some set of "minimum contacts" with the forum state that relate to that cause of action. How to distinguish between general and specific jurisdiction? If the defendant's contacts with the forum state are sufficiently "continuous and systematic", the court may conclude that it has general jurisdiction over the defendant. In that case, the court may assert jurisdiction over the defendant on any cause of action, regardless of whether it arises from the forum contacts. For specific jurisdiction, the defendant's contacts with the forum state need not be so strong, but the cause of action must arise from the forum contacts. [164]

4.9.1.1.3. Enactments of Long-Arm Statute

The principle 'long-arm statute' authorizes the courts to claim personal jurisdiction over a non-resident defendant whose principal business is outside the state on the ground that their action (tortious or any other) falls within the nature of activity required to qualify for jurisdiction. Over a period of time, the States of the US have developed their own respective long-arm statute to exercise personal jurisdiction over any non-domiciliary who commits a tortious act within the state as long as the cause of asserted arises from the tortious act.[165]

4.9.1.1.4. Due Process of Law

The 'due process of law' as given in the Fifth and Fourteenth Amendment of the US Constitution limits the powers of the courts to exercise traditional notions of fair play and substantial justice. The Fourteenth Amendment to the US Constitution provides that "no state shall deprive any person of life, liberty or property without due process of law". The idea is to invoke both long arm statute and due process of law provisions to allow the court to exercise personal jurisdiction over any non-domiciliary defendant.[166]

4.9.1.1.5. Establishing Personal Jurisdiction

The credit to establish ground rules for establishing personal jurisdiction for the non-resident lies with the US Supreme Court judgment in *International Shoe Co.*

---

164 *Ibid.*
165 *Ibid.*
166 *Ibid.*

v. *State of Washington, Office of Unemployment Compensation and Placement ei al*[167] It held that a court's exercise of personal jurisdiction over a non-resident defendant is proper if that defendant has had certain minimum contacts with (the forum state) such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice. It established three criteria for establishing "minimum contacts":[168]

(a) The defendant must "purposeful avail" himself of the privilege of doing business with the forum state,
(b) The cause of action arises from defendant's activities in the forum state, and
(c) The exercise of jurisdiction would be fair and reasonable.

The 'minimum contact' principle laid the foundation of state's jurisdiction over other state's subject. It advocated establishment of 'minimum contacts' to give rise to obligations between the defendant and the forum state. Primarily, it does not look into the issue whether the contacts were sufficient or insufficient to establish "purposeful availment".

4.9.1.1.6. Establishing Personal Jurisdiction in Cyberspace

The courts have been borrowing the principles of personal jurisdiction and extending them to the cyberspace setting. The principles of jurisdiction, which were earlier applied to physical establishments, are now being successfully applied to online business establishments (websites). A website represents a virtual business model. In order to fix the place of jurisdiction, one may have to look into the nature of the website model whether it is 'business oriented' or 'information oriented'. Other key elements that have to be taken into consideration are geographical location of Users, website Owner and web server. Even the terms of service agreements, disclaimers and choice of law or forum clauses play an important role. [169]

4.9.1.1.7. Nature of The Website

An online form of business may exist either in the form of (a) Passive website or (b) Interactive website. As the name suggest, a 'passive' website is meant for information purposes only, whereas an 'interactive' website is a dynamic website and

---

167 326 US. 310.316 (1945).
168 Vakul Sharma, *Information Technology Law and Practice* p.260 (Universal Law Publication Co., 1st edn., 2004).
169 *Id.* at p.261.

provides more than 'mere' information. Application of minimum contacts and long-arm of statute principles have been used by the courts to determine personal jurisdiction by differentiating between ‘passive’ and 'interactive' websites. An important element of minimum contacts is that the contacts need to be of such a character and degree that a defendant could reasonably have expected to be hauled into court in the distant state.[170]

4.9.1.1.7.1. Interactive Websites

In *Cody* v. *Ward*[171], a Connecticut resident brought suit in Connecticut against a California resident, claiming reliance on fraudulent representations made by the defendant resulting in a loss. The Court held that it had valid jurisdiction over the defendant based solely upon bulletin board messages posted by the defendant on an online service’s Money Talk bulletin board and e-mail messages and telephone conversations from the defendant in California to the plaintiff in Connecticut. It simply concluded that the purposeful availment requirement was satisfied by the defendant’s electronic contacts with the plaintiff.

Further, in *CompuServe, Inc.* v. *Patterson*[172], CompuServe, an Ohio corporation with its main offices and facilities in Ohio, sued one of its commercial shareware providers, a resident of Texas. The suit was filed in Ohio and the defendant asserted that the Federal District Court in Ohio lacked jurisdiction over him, claiming never to have set foot in Ohio. The appellate Court measured the defendant's contacts with Ohio and concluded that jurisdiction was proper because: (a) the defendant had purposefully availed himself of the privilege of doing business in Ohio by subscribing to CompuServe and subsequently accepting online CompuServe’s Shareware Registration Agreement (which contained an Ohio choice of law provision) in connection with his sale of shareware programmes on the service as well as by repeatedly uploading shareware programmes to CompuServe's computers and using CompuServe's e-mail system to correspond with CompuServe regarding the subject matter of the lawsuit; (b) the cause of action arose from Patterson's "activities" in Ohio because he only marketed his shareware through CompuServe; and (c) it was not unreasonable to require Patterson to defend himself in Ohio

170 *Ibid.*
171 954 F.Supp.43 (D. Conn.1997).
172 89 F. 3d 1257(6th Cir . 1996).

because by purposefully employing CompuServe to market his products, and accepting online the Shareware Registration Agreement, he should have reasonably expected disputes with CompuServe to yield lawsuits in Ohio.

Similarly, in *EDIAS Software International* v. *BASIS International Ltd.*[173],where an Arizona based software distributor brought suit in Arizona against a New Mexico software development company arising out of the termination of an agreement between the companies and public statements made by the defendant about the termination. The defendant had no offices in Arizona.

4.9.1.1.7.2. Interactive 'Mixed' Websites

Now supposing that if a company maintains a website for the purpose of soliciting business, then would it be called an interactive website. In *Maritz, Inc.* v. *Cybergold, Inc*[174]**,** the court looked at the very basic issue of maintaining a website by the company by framing the due process issue as whether maintaining a website which can be accessed by any internet user and which appears to be maintained for the purpose of and in anticipation of being accessed and used by any and all internet users, including those residing in Missouri (accessed 131 times by residents of the forum state), amounts to promotional activities or active solicitations such as to provide the minimum contacts necessary for exercising personal jurisdiction over a non-resident. The court concluded that because the maintenance of a web site is a more efficient and faster means of reaching a global audience, and through its website, Cyber Gold has consciously decided to transmit advertising information to all internet users, knowing that such information will be transmitted globally.

4.9.1.1.7.3. Passive Websites

In *Bensusan Restaurant Corp.* v. *King*[175], where a New York jazz club operator sued a Missouri club owner claiming trademark infringement, dilution and unfair competition over the use of the name The Blue Note. The defendant maintained a web site promoting his Missouri Blue Note club and providing a Missouri telephone number through which tickets to the club could be purchased. The issue, as framed by the Federal District Court, was whether the existence of the web site was sufficient to vest the court with personal jurisdiction over the defendant under New York's long-

173 947 F. Supp.413 (1996).
174 947 Fsupp.1328 (E.D.Mo. 1996).
175 937 F. Supp. 295 (SDNY,1996).

arm statute. The court considered whether the existence of the web site and telephone ordering information constituted an offer to sell the allegedly infringing product in New York, and concluded it was not. The court noted that, although the web site is available to any New Yorker with internet access, it takes several affirmative steps to obtain access to this particular site, to utilize the information contained there, and to obtain a ticket to the defendant's club.

These steps would include the need to place a telephone call to Missouri and physically travel to Missouri to pick up the tickets ordered. Therefore, the court concluded that any infringement that might occur would be in Missouri not New York. The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York. It found that the defendant did nothing to purposefully avail himself of the benefits of New York. There was no evidence of the defendant actively encouraging New Yorkers to visit the site. The nature of a website whether interactive, mixed or passive depends on the business model the said website is subscribing. It is the degree of interactivity that separates an interactive website from the passive one. The level of interactivity has to take into consideration the purposeful availment of the benefits of the forum state in the form of conducting business online and or offline. [176]

4.9.1.1.8. Sliding Scale Perspective

The judgments as given above reflect the growing acceptance of the fact that the personal jurisdiction depends on the level of interactivity. In *Zippo Manufacturing Company* v. *Zippo Dot Com, inc*[177], the issue of specific personal jurisdiction arose again in the context of a trademark dilution, infringement and false designation under the Federal Trademark Act. Zippo Manufacturing Company, a Pennsylvania based corporation has been well known among other things for Zippo tobacco lighters. Zippo Dot Com, Inc. California Corporation has been providing free news services through its Web site. In addition, the defendant also provided a fee based service to permit the subscriber to view and/or download internet newsgroup messages that are stored on the defendant's server in California. The defendant, a California

---

176 Vakul Sharma, *Information Technology Law and Practice* p.262 (Universal Law Publication Co., 1st edn., 2004).

177 952 F. Supp.1119 (W.D.Pa.1997).

corporation, was sued in Pennsylvania. Court task was to determine whether Dot Com's conducting of E-Commerce with Pennsylvania residents constitutes the purposeful availment of doing business, in Pennsylvania. dot com not only chose to process Pennsylvania residents applications but also assigned them passwords. The court concluded that this level of contact with the state justified the exercise of specific personal jurisdiction.

The court noted that the cases reveal a sliding scale, in which at one end of the spectrum situations where a defendant clearly does business over the internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet, personal jurisdiction is proper. (e.g. Compuserve v. Patterson). At the opposite end are situations where a defendant has simply posted information on an internet Web site, which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. (e.g. BensusanResturant Corp., v. King). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and the commercial nature of the exchange of information that occurs on the Web site.[178]

4. 9.1.1.9. The Effect Test and Online Interaction

Another criterion that has been accepted by the courts has been the effects of online interaction on the forum state. The US Supreme Court in *Calder* v. *jones*[179], held that the "minimum contacts" due process requirement may be satisfied on the basis of the effects that out-of-state conduct has in the forum state. In that case, the Court held that a California court could assert jurisdiction over a Florida publisher that published an article defaming the plaintiff, in view of the facts that plaintiff resided in California. The court reasoned that the defendants had engaged in intentional, and allegedly tortious, actions (that were) expressly aimed at California,

178 *Ibid.*
179 456 U.S.783 (1984).

and that they knew that the brunt of the injury would be felt by the plaintiff in California.[180]

The effect test is a further extension of the 'forum state targeting', as it also takes into consideration the effect that "out-of-state" conduct has in the forum state. Thus, in order to have personal jurisdiction, there must be: (1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which the defendant knows is suffered or likely to be suffered in the forum state. What separates the effect test from other personal jurisdiction approaches is that the focus is on the knowledge or likelihood of causing harm in the forum state. All the previous approaches put more focus on the level of either online or online as well as offline interactions. That is why more and more cases involving defamation or infringement of intellectual property rights have been decided on the basis of this test.

For example, in *Telco Communications* v. *An Apple a Day*[181], (The Virginia plaintiff sued the Missouri defendant for infer alia defamation in internet press releases from Which the plaintiff's tock prices suffered. The court held the exercise of jurisdiction to comport with due process since the defendant knew the statements would be damaging to the plaintiff and was aware of the location of the plaintiff in Virginia); *PurCo Fleet Services, Inc.* v. *Towers*[182], (defendant registered domain name corresponding to plaintiff's trademark, and set up website that forwarded visitors to its own site); *3DO Co.* v. *Pop top Software Inc*[183].'.., (defendant's website allowed visitors to download software that allegedly infringed plaintiff's copyright and misappropriated plaintiff's trade secrets); *Bunn-O-Matic Corp.* v. *Bunn Coffee Service, Inc*[184], (defendant's website included terms that allegedly infringed plaintiffs trademarks); *Digital Equipment Corp.* v. *AltaVista Technology, Inc*[185], (the court drew an analogy between trademark infringement that occurs on a website and infringement that arrives in the state via other means of communication like telex, telephone and mail and held that using the internet under the circumstances of this case is as much knowingly sending into Massachusetts the allegedly infringing and

---

180 Vakul Sharma, *Information Technology Law and Practice* p.262 (Universal Law Publication Co., 1st edn., 2004)
181 Civ. Act.No 97-542 (E.D.Va.1997).
182 38 F.Supp.2d 1320 (D. Utah 1999).
183 49 U.S.P.Q.2d (BNA) 1469 (N.D.CaI1998).
184 46 U.5.P.Q.2d (BNA) 1375 (C.D.IU 1998).
185 960 F.Supp .. 456 (O.Mass 1997).

therefore tortious uses of Digital's trademark as is a telex, mail, or telephonic transmission)."

4. 9.1.1.10. Jurisdiction on The Basis of Online Electronic Contract

Online contracts come with terms of service agreements and disclaimers. These agreements impose restrictions on the users' regarding the choice of law and forum selection. The judicial view as arrived in *Bremen* v. *Zapata Off-Shore Co.*[186], is that such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be unreasonable under the circumstances. This rule applies, under the federal law, both if the clause was a result of negotiation between two business entities, and if it is contained in a form of contract that a business presents to an individual on a take-it-or-leave-it basis.

4. 9.1.1.10.1. Forum Selection Clauses: Click-Trap Contracts

It makes a good legal sense for the online service providers to limit their exposure to one jurisdiction only. Defending lawsuits at multiple locations could be both expensive and frustrating. Thus, the online service provider has no other choice but to subject themselves to only one set of forum and applicable laws only. The user has no other choice, but to accept the service provider's terms of service conditions by clicking an on-screen button that says "I Agree", "I Accept" or "Yes". [187] In *Groff* v. *America Online, Inc*[188], the plaintiff, an individual in Rhode Island who subscribed to America Online, sued the company in Rhode Island state court, alleging violations of state consumer protection legislation. The process of becoming a member of AOL includes a step in which the applicant must assent to AOL's Terms of Service by clicking an "I Agree" button. The Terms of Service "contains a forum-selection clause which expressly provides that Virginia law and Virginia courts are the appropriate law and forum for the litigation between members and AOL. AOL moved to dismiss this suit from the Rhode Island Superior Court for improper venue on the ground that a forum selection clause in the parties' contract mandated that the suit be brought in Virginia, where AOL's base of operations was located. The court agreed, and dismissed the suit. The court held that the plaintiff assented to AOL's terms of service

---

186 407 U.S. 1,9-10 (1972).

187 Vakul Sharma, *Information Technology Law and Practice* p.273 (Universal Law Publication Co., 1st edn., 2004).

188 1998 WL 307001 (R.I. Super. 0.1998).

online by the click of an "I agree" button. The terms of service included a clause mandating that suits concerning the service be brought in Virginia. AOL customers must first click on an "I agree" button indicating assent to be bound by AOL's terms of service before they can use the service. This button first appears on a web page in which the user is offered a choice to either read, or simply agree to be bound by, AOL's terms of service. It also appears at the foot of the terms of service, where the user is offered the choice of clicking either an "I agree" or "I disagree" button, by which he accepts, or rejects the terms of service.

The court held that a valid contract existed, even if the plaintiff did not know of the forum selection clause:

> "*Our Court ... stated the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively "signed" the agreement by clicking "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement."*

It is important to note that in *Groff* v. *America Online, Inc*[189], the court had also taken into consideration the place of execution of the online contract. It opined the place where the transaction has been performed appears to take place where defendant's mainframe is located (Virginia) and not the place (Rhode Island) when plaintiff clicked the "I Agree" button.

4. 9.1.1.10.2. Jurisdiction Based on Location of A Web Server

Asserting personal jurisdiction based on the defendant's use of IT infrastructure of a service provider, located in the forum state, to host its website may also compel the forum state to exercise its jurisdiction over such defendant.[190] In *Jewish Defense Organization, Inc.* v. *Superior Courts,* [191] the plaintiff brought an action for defamation in a California court. Defendants' only relevant contacts with California consisted of contracting with internet service providers, located in California, to host a website, which they maintained from their residence in New York. The court concluded that the defendant's conduct of contracting, via computer,

---

189 1998 WL 307001 (R. I. Super C t. 1998).

190 Vakul Sharma, *Information Technology Law and Practice* p.273 (Universal Law Publication Co., 1st edn., 2004).

191 85 Cal.Rptr.2d 611 (CaI.Ct.App.1999).

with Internet service providers, which may be California corporations or which may maintain offices or databases in California, is insufficient to constitute 'purposeful availment.'

Location of a web server alone cannot be taken as a sufficient cause to constitute 'purposeful availment'. Hosting a website means allotting some space on the web server. One may have to look into the kind of services provided by the web hosting company and the frequency of their utilization by the web promoter to establish 'purposeful availment' of the forum state where the server is located.[192]

4. 9.2. Personal Jurisdiction in Cyber Space: European Union Perspective

Fundamentals of jurisdiction within European countries are based on statute or regulation, instead of constitutional due process applied in case law, as in the U.S. Nonetheless, the results under both systems have a good deal in common. The Brussels Convention is the controlling document for jurisdictional issues within the European Union (E.U.).[193] It sets forth the following basic rules. First, a person who is domiciled in an E. U. member country may be sued in that country. Second, in contract matters, a person may be sued in the place of performance of the obligation in question. Third, a person may be sued in tort matters in the place where the event causing harm occurred. Fourth, a consumer may be sued either only in the consumer's country of domicile, while a consumer may elect to bring an action in his domicile or in the other party's domicile. So long as the consumer was subject to a specific solicitation or advertising in the consumer's domicile. Finally, in entering into contracts not involving a consumer, the parties can agree on a forum for disputes.[194]

Since, jurisdiction in European countries is not limited by constitutional due process as it is in the U.S., the Brussels Convention does not require minimum contacts between the forum and the defendant. The Convention permits assertion of jurisdiction over a defendant if conduct wholly outside the forum resulted in a tort injury to the plaintiff within the forum. In certain instances, at least, E.U. members

---

192 Vakul Sharma, *Information Technology Law and Practice* p.273 (Universal Law Publication Co., 1st edn.,2004).

193 Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters (September 30, 1968).

194 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.844 (Kamal Law House, Kolkata, 1st edn., 2008).

construe their jurisdiction to extend to conduct on the internet that offends policies within the Member State, regardless whether there was intent to cause an effect within that forum.[195]

In the case of *1-800 Flowers Inc. v. Phonenames Ltd.*[196] concerned an appeal against a decision to register the trade mark 800 FLOWERS in class 35 for flowers and floral products. The applicant had argued that the trademark had been used in the UK by its use on a web site. The court considered that merely because an internet web site could be accessed from anywhere in the world, that of itself did not mean that it should be regarded as having been used everywhere in the world. Use, for trade mark purposes, depended on all the circumstances of a particular case, particularly the intention of the owner of the web site and the understanding that a person using the internet would gain from reading the web site. On the facts of this case, the applicant's use of the mark on its website did not sufficiently constitute evidence of the requisite intention to use the mark in the United Kingdom.

In *Euromarket Designs Inc. v. Peters* [197] concerned alleged acts of infringement of a mark registered in the UK by the use of a sign by the defendant on a web site emanating from Ireland. An American company had a UK trademark for 'Crate and Barrel' . The defendant, Peters, ran a store in Dublin called 'Crate and Barrel'. The defendants advertised their shop in Dublin on a web site. It was alleged that two kinds of goods sold in the Irish store, a hurricane lamp and a beaded coaster, fell within the specification of the plaintiff's trademark. The question turned on whether the sign 'Crate and Barrel' on the defendant's web site had been used in the UK. The court considered that an apt analogy was to consider peering down a telescope towards Dublin, and being invited to visit the shop in Dublin. This would not amount to use in the UK. This was different to other internet selling activities, where the web site owner goes out actively seeking world-wide customers. In those circumstances, a sign would be used on a web site. The judge relied on the fact that the advertisement was intended for a local clientele by the trader, seen in combination with the fact that visitors of the site from outside that local area would understand that the web site was not directed at them. This leads inevitably to the conclusion that any

---

195 *Ibid.*

196 *1·800 FLowers Inc* v. *Phonenames LId* (2000) FSR 697.

197 See, *Euromarket Designs Inc.* v. *Peters* (2001) FSR 20.

active use of the trademark in the course of trade is limited to the local area. In November 2000, the French court directed Yahoo! to block internet users in France from auctions selling the memorabilia. Judge Jean Jacques Gomez of the Pans Tribunal de Grande Instance ruled that Yahoo's display of Nazi artefacts in France violated the law and was "an offence against the collective memory of a country profoundly wounded by the atrocities committed by and in the name of the Nazi criminal enterprise.[198]

4.10.2.1. The Brussels Regulation: **An Jurisdictional Aspect**

The Brussels Regulation, which became effective on March 1st, 2002, (The Regulation[199] on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the Electronic Fund Transfer Countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.[200]

4. 9.2.2. Applicability of Brussels Regulation in Cyberspace

The Brussels Regulation has become the established law to resolve disputes concerning jurisdiction and enforcement of judgments in civil and commercial matters. The Regulation is also applicable to resolve online commercial disputes. On the issue of jurisdiction the Brussels Convention (remained unchanged ill the Regulation), sets the rule subject to the provisions of this Convention, persons domiciled in a Contracting State shall, whatever their nationality, be sued in the courts of that State. (Article 2). Furthermore, a person domiciled in a Contracting State may, in another Contracting State, be sued: in matters relating to contract, in the courts for the place of performance of the obligation in question ... (Article 5.1). This means that an individual (including a sole trader or a partner in a business sued on his own) can be sued where his principal residence is. Article 60 provides that the domicile of a company or other association (including a partnership) is where it has its statutory

198 Jennifer M. Hampton, "Experts to Probe Yahoo! Nazi Auctions" E-Commerce Times (August 14,2000)., *available at: http://*www.ecommercetimes.comlperllstory/ 4020.html. (last visited on March 25, 2012).

199 Regulation (EC) No 44/2001 20010 L 121 (January 16, 2001).

200 Vakul Sharma, *Information Technology Law and Practice* p.274 (Universal Law Publication Co., 1st edn., 2004).

seat (i.e., its registered office), its central administration or its principal place of business.[201]

From the point of promotions and sale, the Convention says that the consumer may bring proceedings in his own court against a trader if in the state of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising (Article 13), while the Regulation says that the consumer may sue at home if the trader pursues commercial ... activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State ... (Article 15). As websites are generally accessible from anywhere, thus a trader with a website might said to be directing its activities to all EU countries. In case of a dispute, a consumer has a right under Article 15 to take legal action in his or her home court. Any judgment given there would be enforceable in the trader's own country. Article 15 has broadened the scope of traders' liability, as they can now be sued in foreign courts, i.e. for an online trader defending lawsuits at multiple locations could be both expensive and frustrating.[202]

4. 9.2.3. Rome Convention: **An Jurisdictional Aspect**

To resolve such cross border consumer contractual disputes, the EU Member Slates became signatories to the Rome Convention, 1980. It decides which country law would applies in contractual disputes. The Convention gave freedom of choice to the contracting parties: A contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonable certainty ... (Article 3.1). It further states that the mandatory rules of the consumer's country of habitual residence will always apply whatever choice of law is made (Article 5).[203]

The Convention further provides that in the absence of choice of law the contract is to be governed by the law of the country with which it is most closely connected" (Article 4.1) and it presumes that "the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has ... his habitual residence or ... its central administration (Article 4.2). The performance constitutes the essence of the contract and is generally understood to mean the performance for which the payment is due. It

---

201 *Id.* at p.276.
202 Vakul Sharma, *op.cit.* p.274.
203 *Id.* at p.275.

operates by reference to the country where the party who is to affect the characteristic performance has his habitual residence, or, in the case of a company, its central administration. [204]

4. 9.2.4. Applicability of The Rome Convention in Cyberspace

Both the Brussels and the Rome Conventions highlight a consumer oriented Articles stating that the consumer may bring proceedings against the trader. In the state of the consumer's domicile/ habitual residence, if the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising. The questions are whether these Articles are applicable to an online environment also and do a website promoted by a trader amount to a specific invitation.[205]Applying the Conventions in an online setting would require an interpretation of the phrase preceded by a specific invitation addressed to him or by advertising i.e. whether an internet website constitutes advertising in the state of the consumer's domicile. The answer lies in the nature and form of specific invitation. If the website provides information in the country specific language and offers goods and services in such currency, then it may fulfil the criteria of specific invitation. In such a case, a website is to be seen as the one being directed at that specific country and the consumer can bring proceedings against the trader in their specific (home) country. For example, a website giving information in French and quoting prices in france cannot be said to be directed towards the UK consumers. As far as applicable law is concerned, the courts within the EU apply the Rome convention even where the applicable law is that of a third country or the parties are not resident or established in the EU.[206]

4. 9.3. Personal Jurisdiction in Cyberspace: Indian Perspective

The issue of jurisdiction has to be looked into from two perspectives:

(a) Perspective jurisdiction, and
(b) Enforcement jurisdiction.

Perspective jurisdiction describes a state's ability to define its own laws in respect of any matter it chooses. While a state's enforcement jurisdiction within its own territory is presumptively absolute, gap matters and persons situated thereon.

---

204 *Ibid.*
205 *Id.* at p.276.
206 United State has not agreed to the Rome and Brussels Convention.

Hence, the state legislative enactments primarily reflect its perspective jurisdiction. For example the Information Technology Act, 2000 provides for perspective jurisdiction.[207] Indian courts are authorized to grant injunction or anti-suit injunction to a party over whom it has personal jurisdiction in an appropriate case. This is because court of equity exercises jurisdiction in person. This power is to be used sparingly as though it is directed against a person, but may cause interference in the exercise of jurisdiction by another court. Keeping in view the nature of the online commerce involving business to business, business to customer, customer to business, customer to customer or inter-organizational contracts, it is important that the issue of personal jurisdiction should be looked into from the point of view of following possible sources:

(a) Forum of choice
(b) Civil Procedure Code, 1908, and
(c) Choice of law

Forum of choice indicates that parties may themselves agree beforehand that for resolution of their dispute. They would either approach any of the available courts of natural jurisdiction or to have the disputes resolved by a foreign court of their choice according to the law applicable to that court.[208]

As far as the criminal law is concerned, the position has been straighten by the Information Technology Act, 2000 which says that if the impact of a particular act is felt in India, Indian courts will have jurisdiction, thereby endorsing the 'effect' theory. Looking from a contractual perspective, the law is contained in the Code of Civil Procedure, which says that the jurisdiction lies where the cause of action, whether wholly or partly, arises. This principle would mean even if a part of cause of action has arisen within the precincts or the jurisdiction of an Indian court, the Indian court could exercise jurisdiction. Section 20 of the Code of Civil Procedure does not talk about due process or minimum contact principles. Therefore, under this theory mere Web site access could suffice for a court to assume jurisdiction. The moment a plaintiff shows that the Website is accessible from India; he can show that a part of the cause of action has arisen here because Indian viewers are likely to view the Web

---

207 See, Sec. 75 of The Information Technology act, 2000.

208 Vakul Sharma, *Information Technology Law and Practice* p.278 (Universal Law Publication Co., 1st edn., 2004).

site. Both the Copyright Act, 1957 and the Trade Marks Act, 1999 say that the plaintiff can file a suit where he is located; he does not need to bother about where the defendant is located. This means Indian courts have a very wide jurisdiction as far as the internet is concerned.[209] It is within the power of the Indian courts to grant injunction or anti-suit injunction to a party over whom it has personal jurisdiction in an appropriate case. This is because courts of equity exercise jurisdiction in personam. This power is to be used sparingly as though it is directed against a person, but may cause interference in the exercise of jurisdiction by another court. More so, as the courts have to observe the rule of comity which states that 'the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its law.[210]

However, we find that courts in India are, to a large extent, looking at something beyond mere access of a Web site. In, *Himalayan Drug Company v. Sumit*[211], the plaintiff, the Himalaya Drug Company, had on their Web site a huge database on Ayurvedic concepts and herbs listing out the herbs' Sanskrit and Latin names, their properties, the medicines it was used with graphical and pictorial presentation. The whole database was exactly copied by the defendant who was based in Italy and pasted on a Web site called ayurveda.sumit.net. The only contact with the plaintiff's was the one stated on the Web site in the form of an e-mail address 'sumit@democrat.com'. So, the plaintiff sued the defendant along with the Internet service provider, also an Italian entity, virtualace.net, who had actually sub leased the domain name and Web space to the infringer. The court exercised jurisdiction in this case because it was a case of copyright violation and under Section 62 of the Copyright Act, 1957, a suit can be filed at a place where the plaintiff in based. Moreover the Web site could be opened in Delhi and the damage could also be said to have occurred there. The fact that the defendants belonged to Italy did not desist the court from exercising jurisdiction.

---

209 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.885 (Kamal Law House, Kolkata, 1st edn., 2008).

210 Vakul Sharma, *Information Technology Law and Practice* p.277 (Universal Law Publication Co., 1st edn., 2004).

211 Suit no. 1719 of 2000(Delhi High Court).

Keeping in view the nature of the online commerce involving business-to-business (B2B) or business-to-consumer (B2C) contracts, it is important that the issue of personal jurisdiction should be looked into from all possible sources: (a) forum of choice (b) Civil Procedure Code, 1908 and (c) choice of law.

4. 9.3.1. Jurisdiction: A Forum of Choice

In fact, the parties may themselves agree beforehand that for resolution of their disputes, they would either approach any of the available courts of natural jurisdiction or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. Thus it is open for a party for his convenience to fix the jurisdiction of any competent court to have their dispute adjudicated by that court alone. In other words, if one or more courts have the jurisdiction to try any suit, it is open for the parties to choose any one of the two competent courts to decide their disputes. In case parties under their own agreement expressly agree that their dispute shall be tried by only one of them then the parties can only file the suit in that court alone to which they have so agreed. The growing global commercial activities gave rise to the practice of parties to a contract agreeing beforehand to approach for resolution of their disputes thereunder either any of the available courts of natural jurisdiction and thereby create an exclusive or non-exclusive jurisdiction in one of the available forums or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. It is well-settled principle that by agreement the parties cannot confer jurisdiction where none exists, on a court to which CPC applies, but this principle does not apply when the parties agree to submit to the exclusive or non-exclusive jurisdiction of a foreign court. Thus, it is clear that the parties to a contract may agree to have their disputes resolved by a foreign court termed as a neutral court or court of choice creating exclusive or non-exclusive jurisdiction in it.

Significantly, in *Hakam Singh* v. *Gammon (India) Ltd*[212], the Supreme Court held that: where two courts or more have under the Code of Civil Procedure jurisdiction to try a suit or proceeding, an agreement between the parties that the dispute between them shall be tried in one of such courts is not contrary to public policy. Such an agreement does not contravene Section 28 of the Contract Act. In

[212] (1971) 1 SCC 286.

another significant judgment, the Supreme Court has ruled in *Dhannatal* v. *Kalawatibai*[213], There is no wrong without a remedy (Ubi jus ibi remedium). Where there is a right there is a forum for its enforcement. The plaintiff is dominus litis, that is, master of, or having dominion over the case. In case of conflict of jurisdiction the choice ought to lie with the plaintiff to choose the forum best suited to him unless there be a rule of law excluding access to a forum of the plaintiff's choice or permitting recourse to a forum will be opposed to public policy or will be an abuse of the process of law. It is very much clear from the aforesaid discussion that the forum of choice is discretionary and at the instance of the contractual parties. The parties may submit themselves to the exclusive or non-exclusive jurisdiction of either natural or neutral forum.

4. 9.3.2. Jurisdiction and Code of Civil Procedure

In all civil matters, the Code of Civil Procedure (hereinafter referred to as CPC), 1908, basically formulates the Indian approach to jurisdiction. Under CPC, one or more courts may have jurisdiction to deal with a subject matter having regard to the location of immovable property, place of residence or work of a defendant or place where cause of action has arisen. Where only one court has a jurisdiction, it is said to have exclusive jurisdiction; where more courts than one have jurisdiction over a subject matter. They are called courts of available or natural jurisdiction. The jurisdiction of the courts to try all suits of civil nature is very expansive as is evident from the plain language of Section 9 of the Civil Procedure Code, 1908. This is because of the principle of Ubi jus ibi remedium (there is no wrong without a remedy).

4. 9.3.2.1. Basis of Jurisdiction

To formulate whether the jurisdiction of the courts is exclusive or non-exclusive in the internet setting, one must involve the jurisdictional principles as highlighted in the Civil Procedure Code, 1908:

(a) Pecuniary
(b) Subject-matter
(c) Territory and
(d) Cause of action

[213] (2002)6 SCC 16.

Pecuniary jurisdiction limits the power of the court to hear cases up to a pecuniary limit only. As Section 6 provides "Nothing herein contained shall operate to give any Court jurisdiction over suits the amount or value of the subject matter of which exceeds the pecuniary limits (if any) of its ordinary jurisdiction". It is important to note that subject to the pecuniary or other limitations prescribed by any law, jurisdiction also depends on where subject-matter situate (Section 16), where a suit is for compensation for wrong done to the person or to movable property[214] or where defendants reside or cause of action arises.[215] On one hand, the Section 19 gives an option to the plaintiff to institute the suit at any of the available courts of natural jurisdiction and thus creating an exclusive jurisdiction in one of the available forums, whereas on the other hand, the principle behind the provision of clauses (a) and (b) of Section 20 is that the suit be instituted at a place where the defendant is able to defend the suit without undue trouble. Also, the essential notion of a business, as contemplated by Section 20 is that it is commercial in character. The expression 'carries on business' has a commercial flavour and envisages a commercial enterprise.[216]

In *Rajasthan High Court Advocates' Association* v. *Union of India*[217], the Supreme Court held that the expression "cause of action" has acquired a judicially settled meaning: Compendiously the expression means every fact, which would be

---

214 See, Sec. 19 of the Code of Civil Procedure (CPC), 1908 states..... where a suit is for compensation for wrong done to the person or to movable property, if the wrong was done within tile local limits of the jurisdiction of one court and the defendant resides, or carries on business, or personally works for gain, within the local limits of the jurisdiction of another court, the suit may be instituted at tile option of the plaintiff in either of the said Courts.

215 See, Sec. 20 of The Code of Civil Procedure (CPC), 1908 states..... every suit shall be instituted in a Court within the local limits of whose jurisdiction- (a) the defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, actually and. voluntarily resides, or carries on business, or personally works for gain; or

(b) any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carryon business, or personally work for gain, as aforesaid acquiesce in such institution; or

(c) the cause of action, wholly or in part arises.
(explanation)-A corporation shall be deemed to carryon business at its sole or principal office ill (India) or, in respect of any clause arising at any place where it has subordinate office, at such place.

216 Vakul Sharma, *Information Technology Law and Practice* p.279 (Universal Law Publication Co., 1st edn., 2004).

217 (2001) 2 SCC 294.

necessary for the plaintiff to prove, if traversed, in order to support his Right to the judgment of the Court. Every fact, which is necessary to be proved, as distinguished from every piece of evidence, which is necessary to prove each fact, comprises in cause of action. It has to be left to be determined in each individual case as to where the cause of action arises.

4. 9.3.2.2. Cause of Action and Contractual Obligations

Where the cause of action arises from contract, and the parties have not effectively selected the governing substantive law, the relevant criteria in a choice-of-law analysis are:

(1) the place of contracting,

(2) the place of negotiation of the contract,

(3) the place of performance,

(4) the location of the subject matter of the contract, and

(5) the location of the parties.

The expression 'cause of action' signifies that bundle of facts, which the petitioner must prove, if traversed, to entitle it to a judgment in its favour by the court. One can find a better answer to aforesaid plea in relation to 'cause of action' by referring to a decision of the Apex Court in the case of *Oil & Natural Gas Commission* v. *Utpal Kumar Basu & Others*[218] It was a case where the petitioner learnt about tenders being invited for a particular project at Hazira in Gujarat from advertisements appearing in the Times of India in circulation in West Bengal by reading it at Calcutta, submitted its offer from Calcutta, made representations and also sent fax messages from Calcutta and received reply thereto at Calcutta. A writ petition was filed before the Calcutta High Court on the plea of part of cause of action having arisen at Calcutta. In view of the aforesaid facts, holding lack of jurisdiction on the part of Calcutta High Court, which it had assumed by passing impugned order, while allowing the appeal, the Supreme Court laid down in the following terms: “Merely because it read the advertisement at Calcutta and submitted the offer from Calcutta and made representations from Calcutta would not in our opinion, constitute facts forming an integral part of the cause of action. So also the mere fact that it sent

[218] (1994)4 SCC 711.

fax messages from Calcutta and received a reply thereto at Calcutta, would not constitute an integral part of the cause of action"

4. 9.3.2.3. Choice of Law

Based on its own assessment of the contractual obligations involved, a Court will apply the choice of law rules to determine what law should be applied. The two choices are either to apply the law of the forum (lex fori), or to apply the law of the site of the transaction, or occurrence that gave rise to the litigation in the first place (lex loci). It is obligatory to note that the modern theory of Conflict of Laws recognizes and, in any event, prefers the jurisdiction of the state, which has the most intimate contact with the issues arising in the case. Ordinarily jurisdiction must follow upon functional lines.

In *National Thermal Power Corporation* v. *The Singer Compampany*[219] , the Supreme Court held that: The expression proper law of a contract refers to the legal system by which the parties to the contract intended their contract to be governed. If their intention is expressly stated or if can be clearly inferred from the contract itself or its surrounding circumstances, such intention determines the proper law of the contract. Where, however, the intention of the parties is not expressly stated and no inference about it can be drawn, their intention as such has no relevance. In that event, the courts endeavour to impute an intention by identifying the legal system with which the transaction has its closest and most real connection. The expressed intention of the parties is generally decisive in determining the proper law of the contract. The only limitation on this rule is that the intention of the parties must be expressed bona fide and it should not be opposed to public policy.

Moreover, it was held by the Supreme Court in *Satya v. Teja Singh*[220] that every case which comes before an Indian court must be decided in accordance with Indian law. It is another matter that the Indian conflict of laws may require that the law of a foreign country ought to be applied in a given situation for deciding a case, which contains a foreign element. Such recognition is accorded not as an act of courtesy, but on considerations of justice. It is implicit in that process that a foreign law must not offend our public policy.

---

219 AIR 1993 SC 998.
220 AIR 1975 SC 105-108.

4. 9.3.2.4. Criteria of Accepting Foreign Judgment

A foreign judgment is not conclusive in certain circumstances in India. In this context, Section 13 of the Code of Civil Procedure is relevant and reads:

> *"A foreign judgment shall be conclusive as to any matter thereby directly adjudicated upon between the same parties or between parties under whom they or any of them claim litigating under the same title except-*
>
> *(a) Where it has not been pronounced by a court of competent jurisdiction;*
>
> *(b) Where it has not been given on the merits of the case;*
>
> *(c) Where it appears on the face of the proceedings to be founded on an incorrect view of international law or a refusal to recognize the law of India in cases in which such law is applicable;*
>
> *(d)Where the proceedings in which the judgment was obtained arc opposed to natural justice;*
>
> *(e)Where it has been obtained by fraud; and*
>
> *(f) Where it sustains a claim founded on a breach of any law in force in India."*

The aforesaid clauses from (a) to (f) underlines under what conditions a foreign judgment shall be taken as conclusive. It was observed by the Supreme Court in *Smita Conductors Ltd.* v. *Euro Alloys Ltd,*[221] that a foreign award cannot be recognized or enforced if it is contrary to (1) fundamental policy of Indian law; or (2) the interests of India; or (3) justice or morality. Once it is held that an award is a foreign award-, the provisions of Foreign Awards (Recognition and Enforcement) Act, 1961 would apply and where the conditions for enforcement of such an award exist, the Court shall order the award to be filed and shall proceed to pronounce judgment granting award and upon the judgment so pronounced, decree shall follow. It is now established law that for enforcement of a foreign award there is no need to take separate proceedings, one for deciding the enforceability of the award to make it a rule of the Court or decree and the other to take up execution thereafter. In one

[221] (2001)7 SCC 728.

proceeding the Court enforcing a foreign award can deal with the entire matter. [222] It is obligatory to know that provisions as contained in Section 13 and Section 14, CPC would apply when a suit is brought on a foreign award. Under Section 14, CPC, "the Court shall presume, upon the production of any document purporting to be a certified copy of a foreign judgment, that such judgment was pronounced by a court of competent jurisdiction, unless the contrary appears on the record; but such presumption may be displaced by proving want of jurisdiction". Also, under Section 44A CPC, there is a provision for execution of decrees passed by courts in reciprocating territory. Explanation 1 to this section defines "reciprocating territory" to mean any country or territory outside India which the Central Government may, by notification in the Official Gazette, declare to be reciprocating territory for the purpose of this section. [223]

4.10. Jurisdiction and Information Technology Act, 2000

Cyberspace transactions know no national or international boundaries and are not analogous to three dimensional worlds in which Common law principles developed. Web access is possible from any part of the globe and parties may not be aware about the jurisdictions, which their transactions may traverse. The Common law principles relating to jurisdiction are not readily adaptable to transactions in cyberspace.[224]Due to the near unanimity of the laws applicable throughout India, the only question likely to arise at the national level is the question of jurisdiction of the courts. Jurisdictional issues in India are determined either by the place of residence or place of business test or the cause of action test.[225]The first test is an objective one and easy to determine. It is unlikely to pose any serious issue in E-Commerce disputes. The cause of action test is a subjective test and is most likely to be debated in E-Commerce cases.[226]

The cause of action means every fact, which it would be necessary for the plaintiff to prove, if traversed, in order to support his right to the Judgment of the

---

222 Vakul Sharma, *Information Technology Law and Practice* p.282(Universal Law Publication Co., 1st edn., 2004).

223 *Id.* at p.283.

224 David Thatch, "Personal Jurisdiction and the World Wide Web: Bits (and Bytes) of Minimum Contacts" 23 *Rutgers Computer and Technology Law Journal* p.152 (1997).

225 See, Sec. 20 of The Civil Procedure Code, 1908.

226 Farooq Ahmad, "Electronic Commerce: An Indian Perspective" 9(2) *International Journal of Law and Information Technology* p.157 (2001).

court. It does not include every piece of evidence, which is necessary to prove each fact, but every fact, which is necessary to be proved. Even infinitesimal fractions of a cause of action will be part of the cause of action and will confer jurisdiction on the court within the territorial limits of which that little occurs. It has been made abundantly clear by the Judicial gloss that the formation of the contract is a part of the cause of action and where suit is for damages for breach of the contract, it can lie at any place where the contract was made, notwithstanding that the place where the contract was to be performed and the place where the breach alleged in the plaint occurred, are both outside such Jurisdiction. The place where a contract is concluded will be either the place where acceptance is posted or where acceptance is received depending upon the medium of communication used. However, in case of electronic communications used for executing contracts, place of business or place of residence, as the case may be, will be deemed as a place of contract formation, notwithstanding that the contract may actually be concluded at a different place.[227]

The jurisdiction in Indian criminal courts over matters relating to the internet is somewhat easier to determine. In the first place, the territorial jurisdiction of Indian courts over extra-territorial matters is fairly wide. The offence or any part of it or even the consequences of the offence are factors that the courts would take into account in determining whether they would have jurisdiction over the matter. In general, the principles governing the territorial jurisdiction of criminal courts have been widened considerably in the Indian context, in order that the prosecution of an offence is not hampered solely due to technical grounds, such as the lack of territorial jurisdiction.[228]

While the development of our traditional legal framework requires laws to be circumscribed by territorial restrictions for reasons of sovereignty; legitimacy and effective controls, of the same concerns are irrelevant on the internet. The rise of the global computer network is destroying the link between the geographical location and (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the effort of

---

227 *Ibid.*

228 Tabrez Ahamad, *Cyber law E-Commerce and M-Commerce* p.234 (Publication A.P.H. Publishing Corporation ,1st edn., 2003).

a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.[229]

It is interesting to observe the way India's Information Technology Act, 2000 has addressed the issue of jurisdiction. In what may amount to over Simplification. The Act simply states that it would apply to offences committed or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. This would effectively subject to any web site in the world to the potential jurisdiction of Indian courts. Not only is this unfair it is also unlikely that foreign courts will enforce any order passed by a court in India which have only these provisions as a basis for claiming jurisdiction. This would leave the Information Technology Act, 2000 ineffectual.[230]

The recent Information Technology Act, 2000 passed in India, is illustrative of the prevailing confusion in the area of jurisdiction in the context of the internet. The Act begins by saying, in clause (2) to section 1, that it shall extend to the whole of India and, save as otherwise provided in the Act, it applies also to any offence or contravention there under committed outside India by any person. Clause (2) of Section 75 of the Act also simply states that.... this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Provisions of this nature are unlikely to be effective for a number of reasons.[231]Section 75(1) lays down that the provisions of this Act apply not only for the offences or contravention in India, but they cover the offences so committed outside India also not keeping in mind the nationality of the person committing such offence.[232]Section 75(2) provides that the provisions of this Act shall apply to an offence or contravention provided the act or conduct, which has

---

229 *Id.* at p.235.

230 *Id.* at p.237.

231 Nandan Kamath, *Law Relating To Computers, Internet andE-Commerce* p.52 (Universal Law Publishing Co. Pvt.Ltd., 2nd edn.,(2000).

232 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1094 (Kamal Law House, Kolkata, 1st edn., 2008).

constituted the offence or contravention, involves a computer, computer system or computer network in India. [233]

It is important to note here that though India is not signatory to cyber crime convention, even then it had adopted the principle of universal jurisdiction to cover both cyber contraventions and cyber offences under the Act. Cyber offences involving computer, computer system or computer network have their tentacles spreading in several countries and may create tough jurisdictional problem. In the case, *R. v. Governor of Brixton Prison and another, ex parte Levin,*[234] Citibank faced the attack of a hacker on its cash management system, as a result of which illegal transfer of funds was made from accounts of customers into the hacker's accounts. The said hacker was later on identified and apprehended in the U.K. and deported to the United States. It was held by the Court that real time nature of the communication link between the hacker and the citibank computer meant that hacker's key strokes were actually occurring on the citibank computer.[235]

Firstly, it is unfair to suggest that the moment an Indian computer system is used, an action defined by Indian laws as an offence would be subject to the jurisdiction of Indian Courts. To illustrate, let us consider a web site located in a foreign country. The site may host content that would be perfectly legal in its home country, but may be considered offensive or illegal in India. If an Indian chooses to view this site on a computer situated in India, does that mean that the site can be prosecuted in an Indian Court? This would appear to violate principles of justice. It is to be noted that the judicial trend of examining the amount of activity that a site undertakes in a particular jurisdiction is a far more equitable method to determine jurisdiction. [236] Further, even if Indian Courts are to claim jurisdiction and pass judgments on the basis of the principle expostulated by the Information Technology Act, it is unlikely that foreign Courts will enforce these judgments since they would not accept the principles utilised by the Act as adequate to grant Indian Courts jurisdiction. This would also make the Act ineffective.

---

233 *Ibid.*

234 (1996) 4 All ER, 350 HL.

235 R.K. Chaubey, *An Introduction to Cyber Crime and Cyber Law* p.1094 (Kamal Law House, Kolkata, 1st edn., 2008).

236 Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* p.2 (Universal Law Publishing Co. Pvt.Ltd., 2nd edn.,2000).

In this context, it is necessary that Indian courts take a leaf out of the books of their American counterparts and develop justifiable grounds on which extra-territorial jurisdiction may be validly exercised. The times ahead promise to be very interesting.[237]

Conclusion

When it is examined the crimes in this chapter, there is one fundamental aspect that poses serious problem that is the question of jurisdiction because the nature of the internet is such that geographical and political boundaries has not remain relevant. A person, who can access to a computer and the internet, might be participating, attempting or planning a criminal act anywhere in the globe. In general sense, the internet may be treated as the high seas. No one owns it but people of all nationalities use it. Therefore, cybercrime has become an international issue. Cybercrime has become debated topic across nowadays but our understandings of cyber crime are simultaneously informed and obscured by political and media discussions of the problem. The rapid growth of the internet has created unprecedented new opportunities for offending as well as poses serious challenges for law and criminal justice because it struggles to adapt to crimes that no longer take place in the terrestrial world but in the electronic environment of cyberspace, which span the world through the internet's instantaneous communication, and provide offenders new possibilities for anonymity, deception and disguise.

The emergence of cybercrime raises difficult questions for criminologist of crime ad deviance because these academic disciplines have formed their theories of and explanations for crime on the basis of assumptions drawn from offending in the terrestrial world. But, the virtual environment of the internet is radically different from its terrestrial counterpart; criminology itself is being challenged to adapt its perspectives in order to come to grips with cybercrime or to develop new concepts and vocabularies which may better fit with the digital world. The growth of the internet has become a medium through which copyright industries now claim that illegal copying but the issue of piracy is thus becoming a political and ideological battleground on which the meanings of crime and deviance are negotiated and contested.

---

[237] *Id.* at p.53.

To conclude, it can be said that cyber crime is a new form of crime that has emerged due to the computerization of various activities. With the fast growth of information technology, cyber crimes are increasing leaps and bound with the increase for internet connectivity. The Information Technology Act, 2000 provides penalty for the offences relating to internet to deal with these cybercrime related problem. A tribunal named Cyber Regulation Appellate Tribunal has also been established to provide quick solutions. So, it can be drown conclusion that every possible care is taken by the information technology act to cope up with the problems. Whereas there are still several situations, which is, either not dealt properly or not covered under Information Technology Act, 2000. Hence, there is dare need to frame well equipped national or international legal regulation pertaining to cybercrime.

Cyber Crime means criminal activities taking place in computers and computer networks. knowingly or intentional accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data , computer data base, computer, system, or computer network in order to devise or execute any unlawful scheme, or wrongfully control or obtain money , property or data . Cyber law assimilate the legal, statutory and constitutional provisions that affect computers and computer networks. It concerns individuals, corporate bodies and institutions which:

(1) are instrumental for entry unto cyberspace,

(2) provide access to cyberspace ,

(3) create the hardware and software which enable people to access cyberspace and

(4) use their own computers to go online and enter cyber space.

Major litigants in cyber disputes are telephone provider companies, providers, schools, colleges, universities and final, those individuals, firms and companies that have established a presence on the internet. In present scenario, cyber crime in India is alterations of data are hard realities. The computer needs physical protection. Additional safety measures are needed for computer and the backup information preserved proves an invaluable guide in case of computers crime. Their investigation is highly intricate and daunting. Countries like USA, UK, Germany, Japan, France India have framed laws relating cyber crimes. Consultation of these works can make much better cyber laws to check cyber crime in India and all over the world.

The internet is provides an opportunity where people meet to communicate, where businesses meet consumers and sell their products. In the physical property world, it may be right to the exclusive use of property and the corollary right to exclude all others, which gives value to the property. But in the online world it is the ability of others to access, use, and communicate with the computer which gives value to the network. It is, therefore, is dare need to consider a cyberspace jurisdiction for cyberspace actions which is not feasible effects on real world but the creation, execution and effects are felt only in cyberspace. Cyber Courts and Cyber Arbitral Tribunals must have been given jurisdiction to solve all actions taking place on the internet and the enforcement of their awards and decisions should be made according to international conventions on recognition and enforcement of foreign awards and e-awards. Courts and Arbitral Tribunals should be regarded as equal and independent forms of dispute resolutions.

Generally, there is an option to the parties of contract that they may select a preferred forum, or a preferred choice of law, as a part of their agreements with each other in order to smoothen matters at trial. In the absence of choice-of- law rules, courts may benefit by abiding the wishes of the parties and enforcing valid forum selection clauses. Thus, so far as, issue of jurisdiction in commercial transactions is concerned, it may be advise to create on-line agreements relating to govern those transactions and to mention the jurisdiction in which any disputes will be litigated and the law that will be applied. It should be required that users must manifest their assent to such agreements before they enter into any transactions (in order to help avoid 'shrink wrap' type arguments that the agreements are unenforceable).

The Indian Code of Civil Procedure, 1908, territorial jurisdiction bases on two principles, first, the place of residence of the defendant, and second, the place where the cause of action arises. But there are no guidelines as to how these are to be determined. In the context of the internet, residence of the defendant may include either his place of physical residence, or the place where the web-site server is located. Similarly, the cause of action may be said to arise at a variety of places, where the site is accessed or where its server is located. But in the absence of any statutory clarification, courts will be relied upon precedents.

When it was examined the jurisprudence of both countries in relation to jurisdictional aspects, it revealed some basic premise upon which the treatment of

disputes in those separate jurisdictions is based. In the United States, the courts assumes extra-territorial jurisdiction over a dispute when the defendant fulfils the requirements of the long-arm jurisdiction of the court in which the suit is preferred. But in India, the court assumes jurisdiction over a defendant and how it may be accessed. Now these may seem to be distinct and disparate points of view but when we examine the essential ingredients that must be fulfilled in order to satisfy the requirements of these principles. There are several similarities between them which may allow the Indian courts to assume jurisdiction.

The traditional legal framework based on territorial restrictions for reasons of sovereignty, legitimacy and effective control, becomes irrelevant on the internet because the rise of the global computer network is destroying the link between geographical location and:

(1) the power of local governments to assert control over online behaviour;

(2) the effects of online behaviour on individuals or things;

(3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and

(4) the ability of physical location to give notice of which sets of rules apply.

A Web-site located within a particular jurisdiction may not have impact on the citizens of that location and consequently may remain largely untouched by the laws and regulations of that jurisdiction. Whereas, the persons accessing the 'Web-site from other jurisdictions may seek to impose certain laws and regulations to control the activities of the Web-site but may not be able to do so given the lack of territorial jurisdiction.

Thus, it is proposed to develop of a different new legal boundary in Cyberspace between the real world and the internet. The computer terminal that allows access into the internet would demarcate this boundary and the gateways through this boundary would be through the series of passwords required to enable internet access. Hence, there would not need to ask where a particular offence or event has been committed, as all activities will take place in the realm of Cyberspace. The need to serve notice will not be applied to territorial law, but to the law of the internet and such notice will be served from the moment the password is entered. The issue of jurisdiction has become the international problem where not only the

jurisdiction of the courts but also the applicable law will have to be determined. The problem becomes complicated because of the diversity of the laws applicable. It is possible that any business activity executed over web site may be legal in one country but may not be so in another. Thus, it can be concluded that the issue of jurisdiction applicable law and enforcement of the judgments are not confined to only national boundaries. The issues of jurisdiction at the international level cannot be genuinely addressed by passing national laws because the issue is a global nature and in order to provide homogeneous rules, a global resolution has to be adopted. An international treaty providing uniform rules relating to E-Commerce, jurisdiction of the courts and enforcement of the judgments, needs to be adopted.

CHAPTER V

E-COMMERCE AND THE INTERNATIONAL REGULATION

Introduction

The United Nations Commission on International Trade Law (hereinafter referred to as UNCITRAL) adopted The UNCITRAL Model Law on the Electronic Commerce in 1996 to promote the harmonization and unification of international trade law, whereby remove obstacles to the international trade made by inadequacies and divergences in the law affecting trade. The UNCITRAL has implemented its mandate by formulating the international conventions (United Nations Conventions on Contracts for International Sale of Goods, on the Limitation Period in the International Sale of Goods, on Carriage of Goods by Sea, 1978 (popularly is known as Hamburg Rules), on Liability of Operators of Transport Terminals in the International Trade, on International Bills of Exchange and International Promissory Notes, and on Independent Guarantees and Stand-by Letters of Credit), Model Laws (the UNCITRAL Model Laws on International Commercial Arbitration, on International Credit Transfers and on Procurement of Goods, Construction and Services), the UNCITRAL Arbitration Rules, the UNCITRAL Conciliation Rules, and legal guides (on construction contracts, countertrade transactions and electronic funds transfers).

The Model Law was made to response to a major change in the means of communications which are made between parties using computerized or other modern techniques in doing business (sometimes referred to as trading partners). Similarly, Copyrights, Trademarks and Patents law is known as Intellectual Property. Intellectual Property's importance in Electronic Commerce is difficult to overstate. The internet is a global network of networks through which computers communicate by sending information in packets, and each network consists of computers connected by cables or wireless links. It is the Intellectual Property laws of Copyright, Trademark and Patents that are attempting to harmonize the effects that E-Commerce and the internet have had on the individual's ability to access and use this information.

All country of the world has their own systems for patents, copyrights and trademarks, but due to international coordination and agreement facilitated by the

World Intellectual Property Organization (hereinafter referred to as WIPO) these legal regimes are basically similar in structure and approach. The Electronic Commerce and Intellectual Property Issues is part of WIPO's domain agreement to analises the evolving relationship between the Electronic Commerce and Intellectual Property. The Electronic commerce is at the stages of evolution. The evolution is taking place within the technological and commercial environment characterized by rapid change. The evaluation of the electronic commerce and its relationship with, and effect upon, intellectual property is therefore likely to be an intensive and ongoing process to preserve and enhance the effectiveness of intellectual property in this new digital environment. There would be some discussions as well as some responses that which are either in progress or under consideration and in particular reviews the work of WIPO in this regard.

Fast growing of the internet provides important policy issues relating to both multilateral rules of the international trade and national economic policy. At the multilateral level, the members of the World Trade Organisation (WTO) should decide whether the General Agreement on Tariffs and Trade (GATT) or General Agreement on Trade in Services (GATS) should be applied to the international trade on the internet. It is also be noted that The Directive 2000/31/EC is called the E-Commerce Directive or the Directive on E-Commerce. Although, several other Directives deal solely with e-commerce topics, Directive 2000/31/EC governs core issues regarding Electronic Commerce, e.g. commercial communications, formation of online contracts, and liability of intermediaries. The Directive deals with the central issues of E-Commerce, reason why the Directive is also known as the legal framework directive.

Last 10 years, the internet has fasly removed geographic barriers and revolutionized the way the world communicates. The Georgia Legislature has recently passed the Uniform Electronic Transactions Act, 1999. Georgia is the 47th state to adopt The Act provides some guidance and uniform standards for enforceability of the electronic transactions. Importantly, the Act is voluntary and does not require parties to conduct business electronically. For it to apply, parties must intend to conduct transactions electronically.

5.1. UNCITRAL Model Law on Electronic Commerce

The United Nations Commission on International Trade Law was adopted in June 1996 the Model Law on Electronic Commerce. The Model Law is aim to facilitate Electronic Commerce by providing internationally acceptable rules and legal principles that may be used by the States in enacting legislation to remove legal uncertainties arising from the application of paper-based rules and regulations in the electronic environment. The Model Law is accompanied by a 'Guide to Enactment' that aims to provide national legislators and users of Electronic Commerce with further explanations about the meaning and intent of the provisions of the Model Law. It well establishes the principle that the information should not be denied legal validity and enforceability simply because it is provided in the electronic form. It also sets out requirements that should be met by the data message in order to be treated as equivalent of 'writing', 'signature' and 'original'. In other words, it adopts the 'functional equivalent approach', which is based on an analysis of the purposes and functions of the traditional paper-based requirements with a view to determining how those purposes or functions could be fulfilled through electronic means.[1]

The term 'Electronic Commerce' itself has not been defined anywhere in the modal law. Instead, the term 'Electronic Data Interchange' (hereinafter referred to as EDI) has been defined in art 2(b) as follows:(b) 'Electronic Data Interchange (EDI)' means electronic transfer from the computer to computer of information using an agreed standard to Structure the formation.

UNCITRAL Model Law on Electronic Commerce defines electronic data interchange (EDI) as the electronic transfer from the computer to computer of information using an agreed standard to structure the information. Businesses accept that EDI facilitates trade and offers enormous commercial benefits. Among other things, EDI saves time and money by reducing or eliminating expenditure on costs, postage and storage requirement. Typical applications of EDI include purchase orders, invoices and pricing schedules.[2]

---

1 United Nations Conference on Trade and Development: Electronic: Commerce and Development, *available at: http://*www.unctad.orgenDocsposdtem11.en.pdft (last visited on April 5, 2013).

2 Z. A. Zainol, "Electronic Data Interchange (EDI) and Formation of Contract: A Malaysian Perspective" 7(3) *International Journal of Law and Information Technology* pp.256-69 (1999).

The wide definition of the term has been prompted by a recognition of the fact that in certain cases ' E-Commerce ' can be deemed encompass telex and telecopies as well. For example, in certain circumstances, even though the message may have been originated and transferred between parties in the form of an electronic message, it may ultimately have been delivered to the recipient in the form of a facsimile copy or telex printout. These transactions must necessarily be covered within the ambit of Electronic Commerce (or EDI) as well.

5.1.1. The Principles of Non-Discrimination

Article 5 and Art 5 bis[3] of UNCITRAL Modal Law on Electronic Commerce stipulate the process to be adopted in granting recognition to the data messages .

Article 5 Legal recognition of data messages.

> *"Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."*

Article 5 bis. Incorporation by reference.

> *"the Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in data message purporting to give rise to such legal effect, but is merely referred to in that data message."*

Article 5 of the UNCITRAL Modal Law on Electronic Commerce indicates that information would not be denied validity on the sole ground that such information is presented or retained in an electronic form. This does not mean that all data messages, are valid and enforceable but that if they are to be declared invalid, they must be so declared on the basis of considerations other than the fact that they are data messages.[4] Article 5 of the UNCITRAL Modal Law on Electronic Commerce contains the fundamental principle that the data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is be noted, however, that the principle is not intended to override any of the requirements contained in Articles 6 to 10. These

---

3 See, UNCITRAL Modal Law on Electronic Commerce Adopted on June 1998.

4 Rahul Malthan, *op.cit.*p. 182.

Articles laid down that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message.[5]

Article 5 bis of the UNCITRAL Modal Law on Electronic Commerce is a relatively new inclusion into the Model Law. It seeks to address the legal repercussions of incorporation by reference, a term that is used to describe the practice of referring in a given document to terms contained in other documents. While there is no prohibition in law against this practice, the incorporation of this Article as a separate provision in the Model Law, indicates the special importance of the concept of incorporation by reference in the context of E-Commerce. The best example of this is evident in the manner in which email messages are exchanged. More often than not, the email one receives is actually a single email, which is made up of a number of individual messages that were consecutively added to by subsequent parties. These email messages are rarely detailed documents, and contain little more than references to earlier email messages. The provisions of this Article acknowledge this aspect of the electronic age.[6]

Standards for incorporating data messages by reference into other the data messages may also be essential to the use of public key certificates, because these certificates are generally brief records with rigidly prescribed contents that are finite in size. The trusted third party who issues the certificate, however, is likely to require inclusion of relevant contractual terms limiting its liability. The scope, purpose and effect of a certificate in commercial practice, therefore, would be ambiguous and uncertain without external terms being incorporated by reference. While, Electronic Commerce uses the system of incorporation by reference, the accessibility of the full text of the information being referred to may be considerably enhanced by the use of electronic communications. For example, a message may have contained in the uniform resource locators (hereinafter referred to as URLs), which may direct the reader to the referenced document. Such URLs can provide 'hypertext links' to the reader to use a pointing device (such as a mouse) to select a key word which is associated with the URL. The referenced text would then be displayed. In assessing

---

5 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: United Nation, New York (1999)., *available at:http://*www.uncitral.orgp dfenglishtextselectcom05-89450_Ebook.pdf (last visited on June 15, 2013).

6 Rahul Malthan, *The Law Relating to Computers and The Internet* p.184 (Butterworths ,India 1st edn., 2000).

the accessibility of the referenced text, factors to be considered may include as availability (hours of operation of the repository and ease of access), cost of access, integrity (verification of content, authentication of sender, and mechanism for communication error correction), and the extent to which that term is subject to later amendment (the notice of updates and notice of policy of amendment).[7]

5.1.2. The Principles of The Functional Equivalence

The Model Law relies on the 'functional equivalent approach' which is based on the analysis of purposes and functions of the traditional paper-based requirement with a view to determine how those purposes or functions could have fulfilled through Electronic Commerce Techniques. For example, the paper document served main function as the following: to provide that the document would be legible by all; to provide that the document would remain unaltered over time; to allow for reproduction of a document so that each party would hold a copy of the same data; to permit authentication of data by means of a signature; and to provide that the document would be in a form acceptable to public authorities and courts. It is be noted that in respect of all of the above mentioned functions of paper, electronic records may provide the same level of security as paper and in some cases, a much higher degree of reliability and speed, specially in the respect to the identification of source and content of the data, provided that a number of the technical and legal requirements should be met.[8]

However, the adoption of the functional equivalent approach should not be in such way imposing on users of the Electronic Commerce more stringent standards of security than in the paper-based environment. The Model Law adopted a flexible standard, taking into account several layers of existing requirements in a paper-based environment: when adopting the 'functional-equivalent' approach, attention was given to the existing hierarchy of form requirements, which provides distinct levels of reliability, traceability and inalterability with respect to paper-based documents. For example, the requirement that the data be presented in written form (which constitutes

---

7 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: United Nation, New York (1999)., *available at:http://*www.uncitral.orgpd fenglishtextselectcom05-89450_Ebook.pdf (last visited on June 15, 2013).

8 *Ibid.*

a 'threshold requirement') is not to be confused with more stringent requirements such as 'signed writing', 'signed original' or 'authenticated legal act'.[9]

5.1.2.1. Writing

Article 6 of the Model Law stipulates certain suggestions as to how existing law stipulating the requirement for written documents could be amended to embrace E-Commerce.

> **Article 6 Writing** *(1) Where the law requires information to be in 'writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.*
>
> *(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing....*

Article 6 defines the basic standard to be met by a data message in order to consider as meeting a requirement (which may result from statute, regulation or judge-made law) that information is retained or presented 'in writing' (or that the information be contained in a "document" or other paper-based instrument). It is be noted that Article 6 is part of a set of three Articles (Articles 6, 7 and 8), which share same structure and should be read together. In the preparation of the Model Law, special attention was paid to the functions traditionally performed by various kinds of 'writings' in a paper-based environment.[10]

The following non exhaustive list indicates reasons why national laws require the use of 'writings': (1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves.(2) to help the parties be aware of the consequences of their entering into a contract, (3) to provide that a document would be legible by all, (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction, (5) to allow for the reproduction of a document so that each party would hold a copy of the same data, (6) to permit the authentication of data by means of a signature, (7) to provide that a document would be in a form acceptable to public authorities and courts, (8) to

---

9 *Ibid.*

10 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: United Nation, New York (1999)., *available at:http://*www.uncitral.orgpdfenglish textselectcom05-89450_Ebook.pdf (last visited on June 15, 2013)

finalize the intent of the author of the 'writing' and provide a record of that intent, (9) to allow for the easy storage of data in a tangible form, (10) to facilitate control and sub-sequent audit for accounting, tax or regulatory purposes, and (11) to bring legal rights and obligations into existence in those cases where a 'writing' was required for validity purposes. [11]

The word 'usable' is not intended to cover only human use but also computer processing. As to the notion of 'subsequent reference', it was preferred to such notions as 'durability' or 'non-alterability', which would have established too harsh standards, and to such notions as 'readability' or 'intelligibility', which might have constituted subjective criteria.[12]

5.1.2.2. Signature

Technology has provided an alternative. Digital signatures, if used carefully and consistently, can provide a reliable and accurate indication of the authenticity of electronic documents. Since the encryption used in respect of digital signatures is of such a high order of complexity that messages which have been encrypted using a digital signature are not capable of being decoded within a useful time frame, if used consistently, this technology may be even safer than traditional signatures. The Model Law recognises the validity of digital signatures.

Article 7 Signature-

> *(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:*
>
> *(a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and*
>
> *(b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated in the light of all the circumstances, including any relevant agreement.*
>
> *(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature*.

---

11 *Ibid.*
12 *Ibid.*

Thus, Article 7 of the draft law establishes the general conditions under which data messages should be regarded as having been authenticated with sufficient credibility, as to be enforceable in the context of signature requirements of existing laws. It allows a broad definition of what would constitute a signature by stating that any law which states that the signature of any person is necessary shall be deemed to have been satisfied, so long as a method is used to identify that person and to indicate his approval of the message. By refraining from specifying what constitutes the method of identification, the Model Law allows room for advances in technology.[13]

In determining whether the method used under paragraph (1) is appropriate, legal, technical and commercial factors which may be taken into account include the following: (1) the sophistication of equipment used by each of the parties, (2) the nature of their trade activity, (3) the frequency at which commercial transactions take place between the parties, (4) the kind and size of transaction, (5) the function of signature requirements in the given statutory and regulatory environment, (6) the capability of communication systems, (7) compliance with the authentication procedures set forth by intermediaries, (8) the range of authentication procedures made available by any intermediary, (9) compliance with the trade customs and practice, (10) the existence of insurance coverage the mechanisms against unauthorized messages, (11) the importance and value of the information contained in the data message, (12) the availability of alternative methods of the identification and cost of implementation, (13) the degree of acceptance or non-acceptance of the method of identification in relevant industry or field both at the time the method was agreed upon and time when the data message was communicated and (14) any other relevant factor.[14]

5.1.3. The Principles of The Technological Neutrality

The Model Law provides essential procedures and principles to facilitate the use of modern techniques for recording and communicating information in several types of circumstances. However, the framework law which does not itself set forth all the rules and regulations which may be necessary to implement those techniques in an enacting State. Furthermore, the Model Law covers every aspect of the use of

---

13 Rahul Malthan, *The Law Relating to Computers and The Internet* p.187 (Butterworths, India 1st edn., 2000).

14 *Supra note.*8.

Electronic Commerce. Accordingly, an enacting State can wish to issue regulations to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in enacting State, without compromising objectives of the Model Law. It is recommended that, it decide to issue such regulation, an enacting State should give specific attention to need to maintain the beneficial flexibility to the provisions in the Model Law.[15]

The UNCITRAL Model Law on the Electronic Commerce ('Model Law') is a generic law that can be extended and enhanced by individual countries should they so wish. In devising the Model Law, UNCITRAL set out to develop rules that could be used in all countries regardless of their technological proficiency. This automatically preempted the possibility of developing sui generis rules which are sensitive to the full possibilities of electronic technology. The Model Law provides that the electronic communications should be given equivalent the legal effect to paper-based communications and specifically addresses how certain types of electronic communications could substitute for existing paper-based means to satisfy requirements of writing, signatures and contract formation.[16]

5.1.3.1. Originality of the Data Massage

The word 'original' is commonly thought of as referring to the medium on which information was fixed for the first time. If this definition were to be applied, it would have no significance in the context of data messages or the internet, since the essence of the data message is that it is not fixed on any medium, in a form that is intelligible to the ordinary user. [17] However, if one examines why original documents are usually called for, it is evident that this requirement stems from the need to assure the person relying on the document that the document presented has not been altered by any intermediate person. If there is even the slightest doubt that the document has been altered or tampered with, it loses its value as a reliable document. However, if this is the only utility of an original document, it is clear that present technologies

---

15 Andrew Phang, Daniel Seng, "The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code" 7(2) *International Journal of Law and Information Technology* pp.106-107 (1999).

16 Samtani Anil, " Electronic Commerce in Asia: The Legal, Regulatory and Policy Issues" 9(2) *International Journal of Law and Information Technology* pp.93-114 (2001).

17 Rahul Malthan, *The Law Relating to Computers and The Internet* p.188 (Butterworths ,India 1st edn., 2000).

used consistently, can ensure the same level of reliability. This is what is sought to be addressed in Article 8 of the Model Law.[18]

Article 8 is regarded as stating the minimum acceptable form requirement to be met by the data message for it to be considered the functional equivalent of an original. The provisions of Article 8 should be considered as mandatory, to the same extent that existing provisions concerning the use of paper-based original documents would be regarded as mandatory. The indication that the form requirements stated in Article 8 are to be considered as the 'minimum acceptable' should not, however, be construed as inviting States to establish requirements stricter than those contained in the Model Law.

Article 8. Original

> *(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:*
>
> *(a) There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and*
>
> *(b) Where it is required that information be presented that 'information is capable of being displayed to the person to whom it is to be presented. (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.*
>
> *(3) For the purposes of subparagraph (a) of paragraph (1):*
>
> *(a) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and*
>
> *(b) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.*

Article 8(3)(a), by making referring to additions to the original data message refers to computer generated text automatically appended to text messages, digital

[18] *Id.* at p.189.

signatures and other forms of certification that may not be part of the message as originally drafted. This clause makes it clear that so long as the additions do not alter the original text, the fact that additions have been made, would not affect the originality of the message. If these items were added to an original written document, it is likely that they would change its character and may therefore render it unreliable.[19]

5.1.3.2. Admissibility and Evidential Value of Data Messages

The model code also addresses other issues that are areas of concern from the point of view of the legal implications of Electronic Commerce. Article 9 of the model code specifies the circumstances under which data messages would be admissible as evidence.

Article 9. Admissibility and evidential weight of data messages

> *(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:*
>
> *(a) On the sole ground that it is a data message; or*
>
> *(b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.*
>
> *(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability or the manner in which the data message was generated, stored or communicated to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.*

The purpose of Article 9 is to establish both the admissibility of data messages as the evidence in the legal proceedings and their evidential value. In respect to the admissibility, paragraph (1), establishing that the data messages should not be denied admissibility as evidence in the legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in Article 4 and is needed to make it expressly applicable to admissibility of evidence, an area in which

[19] *Supra note.*8.

particularly complex issues might arise in certain jurisdictions. The term 'best evidence' is a term understood in, and necessary for, certain common law jurisdictions. However, the notion of 'best evidence' might rise a great deal of uncertainty in legal systems in which such a rule is not known. States which the term would be regarded as meaningless and potentially misleading may wish to enact the Model Law without the reference to the 'best evidence' rule contained in paragraph (1). As regards the assessment of evidential weight of the data message, paragraph (2) provides useful guidance as to how the evidential value of the data messages should be assessed (e.g., depending on whether they were generated, stored and communicated in the reliable manner).[20]

5.1.3.3. Retention of Data Messages

Article 10 establishes a set of alternative rules for requirements relating to the storage of information that may constitute obstacles to the development of modern trade. Paragraph (1) is intended to set out the conditions under which the obligation to store data messages that might exist under applicable law would be met. Subparagraph (a) reproduces the conditions established under Article 6 for a data message to satisfy a rule which prescribes the presentation of' writing'. Subparagraph (b) emphasizes that the message does not need to be retained unaltered so long as the information stored accurately reflects the data message as it was sent. Subparagraph (c) is intended to cover all information that may need to be stored, which includes, apart from the message itself, certain transmittal information that may be necessary for identification of the message.[21]

5.1.4. Legality and Formation of Electronic Contract

The formation of the Electronic Contract and enforceability of the Electronic Contract is always key issues in the digital environment. It is therefore law relating to Electronic Contract is to be discussed as below.

---

20 *Ibid.*

21 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: United Nation, New York (1999)., *available at:http://*www.uncitral.orgpdfenglish textselectcom 05-89450_Ebook.pdf (last visited on June 15, 2013).

5.1.4.1. Formation and Validity of Electronic Contracts

Chapter III of the Model Law deals with another interesting and important aspect of E-Commerce, the law relating to the formation and operation of contracts concluded electronically.

Article 11. Formation and Validity of Contracts.

> *(l) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.*

What is also perhaps relevant to consider is the use of the phrase 'unless otherwise agreed by the parties in sub-clause (1) of Article 11. This clause allows the parties to the contract to choose whether or not they want to conclude contracts electronically. It therefore does not impose a standard on the parties which either one of them may not be comfortable employing.[22] It is be noted that paragraph (1) reinforces, in the context of contract formation, a principle already contained in some other Articles of the Model Law such as Articles 5, 9 and 13 which establish the legal effectiveness of the data messages. Therefore, paragraph (1) is needed since the fact that electronic messages may have legal value as the evidence and the produce a number of effects, including those provided in Articles 9 and 13, does not necessarily mean that they can be used for the purpose concluding valid contracts. Paragraph (1) covers merely the cases in which both offer and the acceptance are communicated by the electronic means and cases in which only the offer or only the acceptance is communicated electronical form. The time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to the contract formation.[23]

5.1.4.2. Recognition by Parties of Data Messages

Article 12 was added at a later stage in the preparation of the Model Law, in recognition of the fact that Article 11 which was limited to dealing with the data

---

22 Rahul Malthan, *The Law Relating to Computers and The Internet* p.181 (Butterworths, India 1st edn., 2000).

23 *Supra note.*8.

messages which were geared to the conclusion of a contract, and that the draft Model Law does not contain specific provisions on the data messages that related not to the conclusion of contracts but to the performance of the contractual obligations. Since, modern means of communication are used in the context of the legal uncertainty, in the absence of specific legislation in almost countries, it was considered appropriate for the Model Law not to establish the basic principle that the use of the electronic communication should not be discriminated against as expressed in Article 5, and also to include certain illustrations the principle. The Contract formation which is one of the areas where such an illustration is useful. The legal validity of unilateral expressions of will, as well as other notices or statements that may be issued in the form of data messages, also needs to be mentioned.[24]

5.1.4.3. Attribution of Data Messages

In the context of contract formation, the appropriate and accurate attribution of the data message is important for both parties.

Article 13. Attribution of data messages.

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) By a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) By an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) In order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

[24] *Ibid.*

(b) The data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure that the data message was a duplicate.

Clause 3 of this Article relates to circumstances under which the addressee may deem the message to have been sent by the originator. Under the model law, so long as the originator of the message agreed to authenticate a message using a given authentication method, the message will be deemed to have been sent by the originator, if the receiver can verify that it has been sent, by using that authentication method. The authentication method referred to in this clause may be the use of digital signatures, dual key encryption or even a simple password authentication system that is known only to the two parties. The addressee would be entitled to act on the

assumption that the data message was sent by the person who purports to have sent it, unless the sender issues the receiver a notice to the contrary.[25]

5.1.4.4. Acknowledgement of Receipt

The Article 14 are based on assumption that acknowledgement procedures are to be used at the discretion of originator. Article 14 deal with the legal consequences from sending an acknowledgement of receipt, apart from establishing receipt of the data message. The purpose of paragraph (2) is to validate acknowledgement by any communication or conduct of addressee (e.g., the shipment of goods as acknowledgement of receipt of a purchase order), where the originator has not agreed with the addressee that the acknowledgement should be in a particular form. The situation where the acknowledgement has been unilaterally requested by the originator to be given in a specific form is not expressly addressed by Article 14, which may entail as a possible consequence that a unilateral requirement by the originator as to the form of acknowledgements would not affect the right of the addressee to acknowledge receipt by any communication or conduct sufficient to indicate to the originator that the message had been received.

Paragraph (3), which deals with situation where the originator has stated that the data message is conditional on receipt of an acknowledgement and applies whether or not the originator has specified that the acknowledgement should be received by a particular time.[26]The rebuttable presumption established in paragraph (5) is needed to create certainty and would be especially helpful in context of the electronic communication between parties which are not linked by a trading-partners agreement. The second sentence of paragraph (5) should be read in conjunction with paragraph (5) of Article 13, which establishes the conditions under which, in case of an inconsistency between the text of the data message as sent and the text as received, the text as received prevails.[27]

5.1.4.5. Time and Place of Dispatch and Receipt of the Data Messages

---

25 Rahul Malthan, *The Law Relating to Computers and The Internet* p.192 (Butterworths, India 1st edn., 2000).

26 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: United Nation, New York (1999)., *available at:http://*www.uncitral.orgpdfenglish textselectcom05-89450_Ebook.pdf (last visited on June 15, 2013).

27 *Ibid.*

The internet knows no geographical boundaries, it is important that the question of how one would determine 'place' in the context of electronic transactions, has added significance.

Artcle 15. Time and place of dispatch and receipt of data messages.

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) If the addressee has designated an information system for the purpose of receiving data messages receipt occurs:

(i) At the time when the data message enters the designated information system; or

(ii) If the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) If the addressee has not designated an information system, receipt occurs when the data-message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be Received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or where there is no underlying transaction, the principal place of business;

(b) If the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

Sub-clause 1 of Article 15 states that the time of dispatch of a data message is the time when the data message enters in the information system outside the control of the person sending the message. This could be interpreted to mean the message would be deemed to have been dispatched once it enters either the information system of an intermediary (or several intermediaries), or the information system of the addressee. The term 'dispatch' as used in Article 15, is intended to supplement any domestic laws, as may already exist with regard to dispatch of messages and not to displace them.[28]

Paragraph (1) defines the time of dispatch of a data message as the time when the data message enters an information system outside control of the originator which may be information system of an intermediary or an information system of the addressee. The concept of 'dispatch' refers to the commencement of the electronic transmission of the data message. Where 'dispatch' already has an established meaning, Article 15 is supply the national rules on dispatch and not to displace them. If dispatch causes when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous, except where the data message is sent to an information system of the addressee that is not the information system designated by the addressee under paragraph (2)(a).

the paragraph (4) is introduce the distinction between the deemed place of receipt and the place actually reached by the data message at the time of its receipt under paragraph (2). That distinction is not to be interpreted as apportioning risks between the originator and the addressee in case of damage or loss of a data message between the time of its receipt under paragraph (2) and the time when it reached its place of receipt under paragraph (4). Paragraph (4) merely establishes an irrebuttable presumption regarding a legal fact, to be used where another body of law (e.g., on formation of contracts or conflict of laws) require determination of the place of receipt of a data message.[29]

---

[28] Rahul Malthan, *The Law Relating to Computers and The Internet* p.181 (Butterworths, India 1st edn., 2000).

[29] *Supra note.*8.

5.2. E-Commerce: World Intellectual Property Organization (WIPO)

Intellectual Property's importance in Electronic Commerce is hard to overstate. The internet has been defined as a global network of networks through which computers communicate by sending information in packets, and each network consists of computers connected by cables or wireless links. It is the Intellectual Property laws of Copyright, Trademark and Patents that are attempting to harmonize the effects that E-Commerce and the internet have had on the individual's ability to access and use this information. It should be remembered that most countries have their own systems for patents, copyrights and trademarks, but thanks to international coordination and agreement facilitated by the World Intellectual Property Organization (hereinafter referred to as WIPO) these legal regimes are basically similar in structure and approach.[30]

E-Commerce, more than other business systems, often involves selling products and services that are based on Intellectual Property and licensing. Music, pictures, photos, software, designs, training modules and systems, etc. can all be traded through E-Commerce, in which case, Intellectual Property is the main component of value in the transaction. Intellectual Property is signifcant because the things of value that are traded on the internet must have protected, using technological security systems and IP laws, or else they can be stolen or pirated and whole businesses can be destroyed.[31]

WIPO recognises the common interests of rights holders and digital network access providers (Internet Service Providers), and promoting cooperation between them. It promotes the use of rights management technologies to enable creators and rights holders to make digital content available which respect individual privacy and respond effectively to users' needs, and to the needs of individuals and institutions in developing the countries for access to the digital information for development purposes.[32]It promotes accessions to the WIPO Copyright Treaty (WCT) and the

---

30 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www. uop .edu. jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

31 *Ibid.*

32 World Intellectual Property Organization (WIPO): Contribution to The World Summit on The Information Society (WSIS), Geneva (February 17, 2003)., *available at http://*swww.itu.intdms_pubitu-smd03wsispc2cS03-WSISPC2-C-0097!!PDF-E.pdf(last visited on February 17, 2012).

WIPO Performances and the Phonograms Treaty (WPPT), both came into force into 2002, in order to ensure that the legal framework is sufficiently robust to meet the challenges of the digital environment.[33]

Finally, E-Commerce is based businesses usually hold a great deal of their value in Intellectual Property. Therefore, the valuation of your E-Commerce business will be affected by whether you have protected your Intellectual Property. Several other E-Commerce companies, like other technology companies, have patent portfolios and trademarks that enhance the value of their business.[34]

5.2.1. WIPO: The Plan of Action Pertaining to The Intellectual Property in The E-Commerce

To convene the World Intellectual Property Organization (hereinafter referred to as WIPO) Summit on the Intellectual Property and Knowledge Economy, in Beijing, China, April 24 to 26, 2003. The WIPO Summit will examine key role of the intellectual property system for creativity and innovation to foster the economic growth and social well-being through wealth creation as well as business development.[35]

The WIPO Standing Committee on Copyright and Related Rights (SCCR) will launch policy discussions and information sharing on the main trends in the copyright and related rights in such fields as applicable law the responsibility of the internet service providers. Collectively these discussions will contribute to more effective protection, development, use, and management of literary and artistic works as well asother objects of protection in the digital environment;[36] Complete the deployment of WIPONET, which provides internet connectivity and Information Technology services for intellectual property offices focusing on the needs of the developing countries whilst providing an e-business platform for the future.

---

33 *Ibid.*

34 Intellectual Property Issues Related to Electronic Commerce under World Intellectual Property Organization (WIPO), Small And Medium-Sized Enterprises Division Geneva Switzerland, *available at http:*//www.wipo.intexportsiteswwwsmeene_ commercepdfip_ ecommerce.pdf (last visited on March 19, 2011).

35 World Intellectual Property Organization (WIPO): Contribution to The World Summit on The Information Society (WSIS), Geneva (February 17, 2003)., *available at http://*swww.itu.intdms_pubitu-smd03wsispc2cS03-WSISPC2-C-0097!!PDF-E.pdf(last visited on February 17, 2012).

36 *Ibid.*

To conduct regional meetings of WIPO Member States, to raise awareness among developing countries in particular concerning Intellectual Property issues raised by E-Commerce, as well as Intellectual Property protection at the national level for the internet domain name system, through country code Top-Level Domains (ccTLDs). These meetings are also aimed at broadening the participation of developing countries in the formation of E-Commerce policies at an international level.[37]

5.2.1. Trademarks in E-Commerce

The rademark is defined, in Section 45 of the Lanham Trade-Mark Act, 1946 as being any word, name, symbol or device or combination thereof that is used by a person or in which a person has a bona fide intention to use in commerce to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source or the goods, even if that source is unknown.[38]Conducting business over the internet also raises jurisdictional issues, with each country potentially applying it's own laws and regulations to the medium. Trademark rights in one country do not generally confer any rights to use that mark in another country. Many countries have developed their own trademark laws that are typically enforceable only within that country.[39] According to the United States Patent and Trademark Office Examination Guide for Domain Names (Examination Guide No.2-99), when a trademark is composed of a domain name neither the URL(http://www.) nor The Trade Level Domain Name (hereinafter referred to as TLD) (.com, .org, .net, .edu) have any significance as an indication of source, since they must be used by every internet site as part of an address.[40]

Most countries have individual systems for protecting trademarks, through a Register of Trademarks. In order to be afforded protection in individual countries a trademark owner must register their mark in each country in which they wish to protect their mark, which can be time consuming and costly. The World Intellectual Property Organization does, however, maintain a system of international trademark

---

37 *Ibid.*

38 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www.uop.edu.jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

39 *Ibid.*

40 *Ibid.*

registration. Two treaties, the Madrid Protocol and the Madrid Agreement Concerning International Registration of Marks <link to Madrid treaties>, govern this process. Members of the Madrid Protocol can apply for international trademark protection based upon a national application. The international application is then filed with WIPO.[41]

5.2.2.1. Domain Names

In the realm of E-Commerce, a company's domain name choice can be a key marketing tool, if not the most important aspect of a company's presence on the net. Users regularly try to guess a company's internet location by typing the name of the company followed by the .com top level domain name. It therefore goes without saying that the proper domain name is a vital element to E-Commerce success.[42]

WIPO, in July 1998, commenced an extensive international process of consultations – "the WIPO Internet Domain Name Process established for the technical management of the domain name system, the Internet Corporation for Assigned Names and Numbers (ICANN), on some questions arising out of the interface between domain names and intellectual property rights.[43]. In the WIPO interim report, it was suggested that consideration be given to the introduction of the non-commercial, use-restricted domain, where the contact details of domain name holders would not be publicly available, as a means of allaying concerns because the public availability of contact details may lead to intrusions of the privacy. In the Report, it is concluded that this idea should be further considered. The Report recommended that ICANN should adopt a uniform dispute resolution policy under which an administrative dispute-resolution procedure is made available for the domain name disputes. In the interim report, it was recommended that the domain name applicants should be required to submit to the procedure in respect of any intellectual property dispute arising out of the domain name registration.[44]

The principal legal concerns surrounding domain names are: (1) the pirating of names, usually through Second level domain (hereinafter referred to as SLD)

---

41 *Ibid.*

42 *Ibid.*

43 Primer on Electronic Commerce and Intellectual Property Issues, World Intellectual Property Organization (WIPO)., *available at http*//:www.ehealth strategies. comfiles_primer.pdf (last visited on March 2, 2013).

44 *Ibid*.

registrations within the .com TLD (Top Level Domains) of a well-known or famous company; (2) the SLD registration of misspelled popular brands; (3) despite the efforts WIPO Worldwide Academy of ICANN, there are still other registries in the world that register confusingly similar marks in various country code TLDs.[45] In *Planned Parenthood Fed'n of Am.* v. *BUCCI*,[46] plaintiff, a nonprofit, reproductive health care organization, registered the service mark Planned Parenthood on the Principal Register of the U.S. Patent and Trademark Office. Defendant, a host of a daily radio program and an active participant in the anti-abortion movement, registered the domain name plannedparenthood.com with a corporation that administered the assignment of domain names on the internet. After registering the name, defendant set up a Web site and home page under the same name. Plaintiff alleged that defendant used plaintiff's mark with the specific intent to damage plaintiff's reputation and to confuse unwitting users of the internet. The court held that the Lanham Act, 15 U.S.C.S. was applicable and that a significant likelihood of confusion existed. Thus, injunctive relief in favour of plaintiff was appropriate. The court granted plaintiff's motion for a preliminary injunction because defendant's use of plaintiff's trademark was subject to the Lanham Act. There was a likelihood of confusion arising from defendant's use of plaintiff's trademark.

If federal trademark registration is desired in the United States for a domain name, an applicant must take into consideration the following situations:

- Advertising one’s own products or services on the internet is not considered as a service. Businesses doing so cannot register a domain name used to identify that activity.
- If a mark is composed solely of a TLD (Top Level Domains) for domain name registry services, federal registration should be refused because the TLD would not be seen as a mark
- Geographic matter may be merely descriptive of services provided on the internet
- If a mark is composed by a surname and a TLD, no registration will be allowed because the mark is merely a surname

---

[45] Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www. uop .edu. jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

[46] 1997 U.S. Dist. LEXIS 3338 (S.D.N.Y. Mar. 19, 1997).

- If a proposed mark is composed of merely descriptive terms combined with a TLD, registration will be refused on the grounds that the mark is merely descriptive
- Marks containing the phonetic equivalent of a TLD are treated in the same manner as marks composed of a regular TLD. For example, the mark XYZ DOTCOM would require the applicant to disclaim the TLD ".COM" rather than the phonetic equivalent "DOTCOM"

<Link to>WIPO – Domain Name Dispute Resolution Service

<Link to> Section 43(d) Cybersquatting Consumer Protection Act

5.2.2.2. Metatags

A Metatag is a keyword embedded in a web site's HTML code as a means for internet search engines to categorize the contents of the web site. Metatags are not visible on the web site itself (although, they can be made visible together with the source code of the page). However, a search engine seeking out all web sites containing the particular keyword will find and list that particular site.[47] The more often the keyword appears in the hidden code, the higher a search engine will rank the site in its search results. In various jurisdictions, trademark owners have challenged the unauthorized use of their trademark as a metatag.[48]

In other contexts, the use of another's trademark as a metatag may be legitimate 'fair use', for example, if a retailer uses a trademark as a metatag to indicate to prospective customers that it is offering the trademarked goods.

5.2.2.2.1. Sale of Trademarks as Keywords.

The web sites of internet search engines are among the most frequented sites on the internet. As such, they are particularly attractive to advertisers. Some of these search engines 'sell' keywords to advertisers who want to target their products to a particular group of internet users. This results in the outcome that, whenever the keyword is entered into search engine, an advertisement appears along with any

---

47 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www. uop .edu. jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

48 Primer on Electronic Commerce and Intellectual Property Issues, World Intellectual Property Organization (WIPO)., *available at http*//:www.ehealthstrategies.comfiles _primer.pdf (last visited on March 2, 2013).

search results. Retailers, for example, have purchased keywords so that their advertisements are displayed whenever it appears that products bearing a particular trademark are being sought. This has been challenged by trademark owners who are concerned that such advertisements might divert customers from their own web site, or from the web sites of their preferred or authorized web retailers. The legal treatment of such cases is, as yet, unclear.[49]

The first case in the United States that held a court enjoined a party from using misleading terms in their hidden text and or meta tags on a website was Playboy, *Enterprises, Inc.* v. *Calvin Designer Label.*[50] The court entered a preliminary injunction enjoining defendant's websites, 'www.playboyxxx.com' and 'playmatelive.com' and repeated use of the 'Playboy', 'Playboy Magazine', and 'Playmate' trademarks in the defendant's meta tags. The defendant had been embedding these trademarked terms several hundred times on web pages in black type on black background so users could not see the reason why the search engines were truly picking up the site. As a result, the defendant's web sites had appeared at the top of most search engine results, often times even before the plaintiff's site <playboy.com>. The law firm of Oppedahl and Larson, an intellectual property firm and owner of the domain name 'patents.com' filed a complaint alleging common law unfair competition and trademark violation and violation of Lanham Act Sections 43(a)(unfair competition) and 43(c)(trademark dilution) after discovering that defendants had used the words "Oppedahl" and "Larson" in the keywords field of their web pages in order to divert web users to their sites. The parties eventually reached a settlement agreement in which the defendant agreed not to use the plaintiff's trademarks in its web pages or meta tags without the plaintiff's prior authorization. Therefore, U.S. courts still have not had an opportunity to speak on a pure meta tags case yet.

5.2.2.3. Linking

One of the fundamental innovations of the internet is its ability to seamlessly connect multiple documents and elements. E-Commerce is better served when a business can connect a user to all the necessary components of a transaction. For example, an internet travel agency not only can provide the user a means to book a

---

49 *Ibid.*

50 985 F. Supp. 1220 (N.D. Cal. 1997).

flight, but the web site can connect the purchaser to other web pages (whether internal or external) so that he may also secure hotel accommodations and even a rental car. This is made possible by tools known as links and frames. Frames can be useful in subordination of documents or establishing an active table of contents. The concern with framing is similar to that of linking. A framing site captures entire web pages from another site into a window on the original site (often times reducing the size of the captured site and any advertisements associated with it). The ability to direct users from one site to another using the hypertext reference links underpins internet commerce and although under some circumstances a party linking to or framing another's site may seek permission, this isn't the norm. Additional problems arise when the framing cuts off the advertising of the linked-to website, or when the framing site surrounds the framed site with its own advertisements. Also, users may not be aware that the framed page belongs to an outside (3rd) party.[51]

In the case of *Washington Post Co.* v. *Total News Inc.*[52], framing was involved. The Total News home page used a table of contents in one frame and a main frame where all the news was displayed. Among others, Washington Post, Reuters and CNN alleged trademark infringement, false designation of origin and unfair competition. The parties settled and Total News agreed to cease framing the plaintiff's web sites in exchange for authorization to link to their sites using hypertext reference links (text only). Each plaintiff was thereby allowed to revoke permission to a link to its site from Total News. If the defendant refuses to remove the link, in order to have the link removed the plaintiff must convince a court that the link in an impermissible violation of rights of intellectual property.

5.2.3. Copyrights in E-Commerce

Web sites are compilations of various components. Much of the material that is used to create or that is found on web sites, such as photographs, text, artwork, and audio components, are copyrightable. Businesses that choose to create an internet presence for themselves need to be aware of how copyright law works and affects material on the web. For E-Commerce businesses, a primary source of protection for

---

51 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http:/*www.uop.edu.jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

52 No. 97 Civ. 1190 (PKL)(S.D.N.Y. filed February 20, 1997).

their intellectual property is copyright law. Material that can be protected through copyright law includes the software that runs programs on the web site, the text and photos on the page, audio components, and databases.

5.2.3.1. Computer Programs Module

Despite the differences between computer programs and more traditional copyrightable works like books and art, the United States Copyright Act, 1976 recognizes computer programs as copyrightable subject matter. As defined in section 101 of the Act, computer programs are a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result. Software can be 'fixed' in a numerous ways such as, source code, object code, diskettes, CD-ROMs, shareware available to be downloaded from the internet, semi-conductor chips, etc. It is well settled in United States law that the literal elements of a computer program are protectable. The literal elements of software include the object and source code.

5.2.3.2. Idea or Expression in Computer Programs

One of the most difficult problems in determining the scope of protection available to software is the separation of the idea behind the program, which is not protectable, from the expression, which is protectable. As with any work of authorship copyright protection only extends to the expression of the work, not the idea behind the work. This is extremely important when determining the scope of protection for computer programs.[53] The Third Circuit in the United States was the first court in the United States to address the issue of whether non-literal copying of a computer program constituted infringement. In *Whelan Associates, Inc.* v. *Jaslow Dental Laboratory, Inc.*[54], the court identified the program's idea broadly as being the purpose of the program and the structure of the program to be protectable expression. The court awarded protection to not just the code, but to the structure, sequence, and organization of the software that was not necessary to the function or purpose of the program.

5.2.3.3. Electronic Rights Management

---

53 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www.uop.edu.jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

54 797 F.2d 1222 (3d Cir. 1986).

To increase the amount of control over copyrighted works, content owners, in the past, have brought together the rights of many parties. For example, the American Society for Composers, Authors and Publisher (ASCAP) and Broadcast Music, Inc. (BMI) handle the non performance dramatic rights licenses for their members. The Harry Fox Agency is responsible for the mechanical rights of numerous music publishers. The recent movement is to increase the amount of control content owners have over their works. This is because the new digital world is presenting new problems in the licensing.[55]

5.2.3.4. Transient Copying

The Digital Millennium Copyright Act (DMCA) also addresses the new issues concerning copying and computer technology. Section 512 of the DMCA creates four limitations on liability for copyright infringement by online service providers. Two of the limitations, among others, include transitory communications and system caching. With respect to transitory communications, the DMCA limits the liability of an online service provider when the provider is simply a conduit for the data.[56]

5.2.4. Patents in E-Commerce

Patents provide an increasingly important form of protection for intellectual property in the E-Commerce arena. This module teaches the basic principles of patent law in the United States system of patents, though references are made to systems from other countries where appropriate.

5.2.4.1. Utility of Patent

E-Commerce across the internet will continue to grow. There are many traditional and non-traditional uses for patents in this rapidly developing sector. The software that runs E-Commerce is a prime target for patenting. So long as the software achieves a useful result and meets all the traditional tests for patentability, a software patent is obtainable.[57]The graphical representations and icons used in the E-

---

55 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://* www.uop.edu.jodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

56 *Ibid.*

57 Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, Franklin Pierce Law Centre, *available at http://*www.uop.edu.JodownloadresearchmembersWIPO.pdf (last visited on May 10, 2013).

Commerce programs may be eligible for design patent protection. Two non-traditional issues of patents particularly deserve discussion; defensive patents and essential facilities. Defensive patenting occurs when a patent is obtained primarily for the purpose of excluding others from an invention, without specifically intending to practice the invention oneself, or when patent is obtained primarily to be used as a bargaining chip in negotiating a license to another's patent. The essential facilities doctrine is implicated when one controls a core technology.

Defensive Patents {link}

Essential Facilities {link}

5.2.4.2. Patents and Its Essential Facilities

With the number of patents being issued and the lack of a competent prior art history against which to compare applications, it is inevitable that some of the core technologies of E-Commerce will receive patents. Once this happens, the question arises whether the patent holder should be forced to allow others a compulsory license to the invention. One such manner in which this might happen is through the doctrine of essential facilities.

5.2.4.2.1. Utility of Patent in the Business Method Patents

Business method patents have set the patent industry on its head and whipped the media in frenzy. Business method patents are fast becoming one of the most important means of protecting E-Commerce assets. The E-Commerce practitioner should have an understanding of the potential benefits and liabilities of these process patents. As we learned in Patentability, a process is patentable subject matter. A process is a series of steps or a method of producing a result, and business method patents are a type of process utility patents.[58]

A business method is defined quite broadly and includes matters not relevant to E-Commerce. The definition is as follows: the business method of (A) administering, managing or otherwise operating an enterprise or organization, including the technique used in doing or conducting the business, or (B) processing financial data (2) any technique used in athletics, instruction, or personal skills, and (3) any computer-assisted implementation of a systematic means described in

[58] *Ibid.*

paragraph (1) or a technique described in paragraph (2). The particular interest to the E-Commerce practitioner is the computer-implemented business method patent. While there is no universally accepted definition, such patents utilize a process to bring about a tangible and useful result relevant to business or commerce by use of a computer. The origin of business method patents predates computer technology, however, and primarily revolves around financial services.[59]

5.2.5. The WIPO Digital Agenda for the Protection of Intellectual Property Rights in the E-Commerce

The WIPO is the organization responsible for the formulation of a policy framework at the international level to encourage creation and the protection of intellectual property and to create theenvironment in which the intellectual property is respected across the world. In this era of rapid technological advancement, the mission of the Organization remains the same.[60]

In September 1999, at WIPO's International Conference on Electronic Commerce and Intellectual Property, Dr. Idris reinforced his initial emphasis with the announcement of the WIPO Digital Agenda. The Agenda's ten points are set forth below:

1. Broaden the participation of developing countries through use of the WIPONET and other means for, access to Intellectual Property information, participation at global policy formulation and opportunities to use their IP assets in E-Commerce.
2. Entry into force of the WCT and the WPPT before December, 2001.
3. Remote adjustment of the international legislative framework to facilitate ecommerce through the extension of the principles of WCT and WPPT to audiovisual works adaptation of broadcasters' rights to the digital era and progress towards a possible international instrument on protection of the databases.

---

59 *Ibid.*

60 Primer on Electronic Commerce and Intellectual Property Issues, World Intellectual Property Organization (WIPO)., *available at http*//:www.ehealthstrategies.comfiles_ primer.pdf (last visited on March 2, 2013).

4. Implement the recommendations of the Report of WIPO Internet Domain Name Process and pursue the achievement of compatibility between identifiers in real and virtual worlds through the establishment of rules for the mutual respect and the elimination of contradictions between the domain name system and the intellectual property rights.

5. Develop appropriate principles for establishing rules to determine the circumstances of intellectual property liability of the Online Service Providers (OSPs) that are compatible as well as workable within a framework of general liability rules for OSPs.

6. Promote adjustment of the institutional framework to facilitate the exploitation of intellectual property in the public interest in a global economy and on a global medium through administrative coordination and, where desired by users, the implementation of practical systems in the respect of, the interoperability and interconnection of the electronic copyright management systems and the metadata of such systems and the online licensing of the digital expression of cultural heritage § the online administration of Intellectual Pproperty disputes.

7. Introduce online procedures for the filing and administration of the international applications for the PCT, the Madrid System and the Hague System at the earliest possible date.

8. Study and respond in a timely and the effective manner according to the need for practical measures to improve the management of cultural, and other digital assets at the international level by investigating the desirability, and efficacy of, model procedures and forms for global licensing of digital assets, the notarization of electronic documents and the introduction of a procedure for the certification of websites for compliance with appropriate intellectual property standards and procedures.

9. Study about other emerging the intellectual property issues pertaining to the Electronic Commerce as well as where appropriate, develop norms in relation to such issues.

10. Coordinate with some other international organizations to formulate the appropriate international positions on horizontal issues affecting Intellectual

Property, in particular and the validity of Electronic Contracts and jurisdiction.[61]

The WIPO Digital Agenda is formulated to update and apply WIPO's mandate to the changes that have resulted from the digital environment, and to facilitate the conduct of Electronic Commerce. The opportunities in this area, as in cyberspace itself, are infinite, provided we continue to meet the challenges head-on.[62]

5.3. E-Commerce: World Trade Organization (WTO)

The World Trade Organization (hereinafter referred to as WTO) became involved with issues of Electronic Commerce. On September 25, 1998, ministers adopted the WTO Declaration on Global Electronic Commerce, which urges the general council to examine all trade-related issues pertaining to global Electronic Commerce. While, the electronic world poses certain challenges to the present trade policy framework, traditional WTO Electronic Commerce. The present framework only roughly provides for those forms of Electronic Commerce changing the global economy. Much effort has been dedicated to involve them into the next round of trade negotiations. As far as dispute resolution is concerned, WTO has a new mechanism for resolving disputes. Generally considered to be a major improvement on the former WTO mechanism, this mechanism came into being after the Uruguay Round of negotiations and has been welcomed by most member states. Importantly, all trade disputes arising out of the WTO framework shall be submitted to this mechanism for resolution. The WTO Dispute Settlement Understanding establishes an integrated dispute settlement system for all multilateral and multilateral agreements under the WTO umbrella. The problem with this mechanism for Electronic Commerce is its exclusive availability to member states. This mechanism is not the one to resolve a private dispute unless, of course, that dispute was supported by a member state.[63] It was decided to have continue with the current practice of not imposing customs duty on electronic transmissions, a decision that was also reviewed at Third Ministerial Conference.

---

61 *Ibid.*

62 *Ibid.*

63 Yun Zhao, *Dispute Resolution in Electronic Commerce* p.63 (Koninklijke Brill NV, Leiden, The Netherlands 1st edn., 2005).

The work programme which involves the relevant WTO bodies was cosidered the economic, financial and development needs of developing the countries and also the work being undertaken in other international fora on this subject. The Geneva Declaration has been formed the basis of zero duty on Electronic Commerce from May 1998 to December, 1999. The Third Ministerial Conference of the WTO at Seattle could not review the work programme relating to E-Commerce. Thereafter, no decision has yet been taken on issue of extending the period of zero duty on the E-Commerce.[64]

5.3.1. E-Commerce and World Trade Organization (WTO)

The degree to which World Trade Organization (hereinafter referred to as WTO) members can regulate. Tax international internet trade will depend on the WTO discipline they decide to apply to it. The WTO report raises the possibility that, in principle, the 'digits' traded on the internet could have viewed as goods, services or even something else. There is no ambiguity regarding to the status of the goods ordered and paid for on the internet but delivered physically in the conventional manner. Except for the order and payment themselves, these transactions are treated as goods trade and the General Agreement on Tariffs and Trade (hereinafter referred to as GATT) discipline applies to them. The ambiguity arises when the goods are delivered on the internet. On the one side of it, any deliveries made by the internet would considered to similar services.

Nevertheless, there are products delivered by internet that have counterparts in merchandise trade. The obvious examples are books, videos, music CDs and computer software. When imported in physical form, these products are treated as goods with the GATT discipline applied to them. Whether they can be treated as services when delivered by internet or, in conformity with their physical counterparts, they should be treated as goods. One extreme possibility is to characterise all transmissions on internet as goods with GATT discipline applied to them. Such a characterisation accompanied by a ban on custom duties on transmissions would amount to the WTO members to complete free trade in transactions routed by internet. This is because national treatment and *most favoured nation* status are general

[64] "Electronic Commerce and Work Programme in WTO", *available at:* http://commerce.nic.in/trade/international_trade_oi_ecommerce.asp (last visited on April 15, 2013).

obligations under GATT. At the national level treatment, the member countries would give up their right to discriminate against the internet imports as far as domestic taxes are concerned. And the ban on custom duty would bind their tariffs on internet imports at zero.[65]

The E-Commerce has developed after the creation of the WTO in 1994. resulting, the WTO does not have any specific Articles for e-commerce. however, there are several WTO agreements related to E-Commerce. These WTO agreements include the General Agreement on Trade in Services (hereinafter referred to as GATS) and the Information Technology Agreement (ITA). The GATS is of particular significance to the E-Commerce for several reasons. First, the communication services that provide access to the E-Commerce fall under the GATS. Second, the execution of electronic transaction necessitates infrastructure services (distribution, payment, etc.) whose liberalization equally falls under GATS.[66]

5.3.2. E-Commerce as A New Dimensional Aspect in The World Trade Organization

E-Commerce has meant the growth of capital productivity through capital augmenting technological change, which in turn is leading to growing supply capacity. All these processes are expected to bring changes in capital and labour markets. Governments in developing countries could have helped improve capital and skills allocation to the technology-sensitive industries. The development of adequate characteristics of human resources which would allow developing countries to benefit from the instruments of ecommerce would be determined by the following demand and supply factors as (a) demand for qualified personnel for employment in private and public sector, (b) inter-firm specialization enhanced by E-Commerce, (c) the ability to practice E-Commerce by individual enterprises and consumers, and (d) the application of selected E-Commerce aspects in social life, including education, medical and government services. Members would continue to keep their current

---

65 Arvind Panagariya, *E-Commerce, WTO and Developing Countries* p.961 (Blackwell Publishers Ltd, Oxford UK, 2000).

66 Bashar H. Malkawi, "E-Commerce in Light of International Trade Agreements: WTO and the United States-Jordan Free Trade Agreement" 15(2) *International Journal of Law and Information Technology* p.156 (2007).

practice of not imposing customs duties on electronic transmissions.[67] In that respect, existing the WTO Agreements were reviewed to create a predictable legal environment and their applicability to the E-Commerce. There was no attempt to define meaning of E-Commerce is, rather what is being traded and what preconditions are necessary for the E-Commerce to take place. Two key areas emerged as especially important to the development of E-Commerce, the General Agreement on Trade in Services and the Agreement on Trade-Related the Intellectual Property Rights. The language in both agreements has been determined as technologically neutral and adequate to trade issues arising from ecommerce.

5.3. 3. Trade in Services Related Issues in The E-Commerce

The service importance in the E-Commerce as internet access services, telecommunication services providing the network access via the internet, and specific services supplied over the internet (e.g. consultancy, telemedicine and distribution services). New services have also risen such as the web hosting, authentication and data 'push' services. That may have not yet raised regulatory concerns. Since, their treatment would come under computer and related services category. The actual product supplied is a good or new the digital product. The Transactions involve distribution services as a component. Which GATS apply to ecommerce raises the question of the electronic transmissions and their service content. One principle is clear that the introduction of E-Commerce into GATS should not consist the level of existing commitments nullifying the level of commitment extended in different sectors.[68]

5.3.4. E-Commerce and Outsourcing

The E-Commerce regardings not only to the cross-border movement of services but also to commercial presence as well as movement of the natural persons. In order to the establishment of a commercial presence by the service provider in host country, this foreign service provider may have also engaged to provide services to its customers, whether domestic or foreign, over the internet. The outsourcing of the software development to other countries, as E-Commerce in the computer-related

---

67 United Nations Conference on Trade and Development: Electronic: Commerce and Development, *available at: http://*www.unctad.orgenDocsposdtem11.en.pdft (last visited on April 5, 2013).

68 *Ibid.*

services, may lead to the establishment of commercial presence as well as may require short-term visits of their service professionals to the customer sites. As a result, the liberalization of the E-Commerce conerning to trade should also include measures affecting (1) commercial presence and (2) presence of natural persons engaged in ecommerce related trade. This would include removal of the economic means.[69]

In that sense, the E-Commerce may render tools to promote economic development ineffective. Additional analysis and introduction of appropriate regulatory instruments may be particularly important in developing countries in order to further advance and use E-Commerce. As a transitory measure, the emergency safeguard measures may be needed in the cases where the E-Commerce related activities create unforeseen developments in the domestic market and More analytical work is necessary before concluding how opening up of market for government procurement through the e-commerce could enhance efficiency and welfare in developing countries. The issues of taxation and consumer protection generally remain outside the GATS and the WTO.[70]

5.4. Electronic Commerce Directive

The Directive 2000/31/EC is popularly called the E-Commerce Directive or the Directive on E-Commerce. Directive 2000/31/EC regulates central issues relating to Electronic Commerce, e.g. commercial communications, formation of online contracts, and liability of intermediaries. The Directive consists of 24 Articles and 65 recitals.[71]The European Parliament adopted On May 4, 2000 the Directive on the Certain Legal Aspects of Information Society Services. Inspite of reservations regarding some individual provisions, the European Parliament has decided to adopt the directive swiftly to the internet's rapid development. Any essential amendments

---

69 United Nations Conference on Trade and Development: Electronic: Commerce and Development, *available at: http://*www.unctad.orgenDocsposdtem11.en.pdft (last visited on April 5, 2013).

70 *Ibid.*

71 Arno R. Lodder, "Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market", *available at: hattp//:*www.SSRNhttpssrn.comabstract=1009945(last visited on May 17, 2013).

will be made to the directive by the amendment clause. On June 8 2000 the directive was published in the *Official Journal* and entered into force.[72]

The development of the Electronic Commerce within the information society offers significant employment opportunities in the Community, specially in small and medium-sized enterprises, and will stimulate the economic growth and investment in innovation by European companies. It can also enhance the competitiveness of European industry. Provided that everyone has access to the internet. Community law and characteristics of the Community legal order are important asset to enable European citizens as well as operators to take full advantage. Therefore, this Directive has the purpose of ensuring a high level of Community legal integration to establish a real area without the internal borders for information society services. It is be noted that Electronic Commerce could fully benefit from the internal market an, therefore, as the Council Directive 89/552/EEC of October 3, 1989 on coordination of certain provisions laid down by law, regulation or administrative action in Member States.[73]

5.4.1. The Objectivity of The Directive

The Directive's main objective is to contribute to ensure the proper functioning of the internal market by ensuring, particularly the free movement of information society services between the Member States[74]. It is impossible to ensure the smooth functioning of the internal market in such an open, global environment as the internet. In the recitals the inherent global nature of information society services is recognised. Recitals 61-62 express that negotiation with third countries is necessary to make laws and procedures compatible and that cooperation with third countries should be strengthened. Also, the Directive does not apply to services by a third country, and is without prejudice to results of discussions by international organisations (UNCITRAL, OECD) on legal issues.[75] However, the creation of an appropriate European regulatory framework may establish a strong negotiation

---

72 "The Impact of the European E-commerce Directive", a*vailable at: hattp//:*www. internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe #applicable (last visited on May 18, 2013).

73 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu~mr2651ecommerce31st StatutesElectronic CommerceDirective.pdf (last visited on June 20, 2013).

74 Article 1(1) of The DIRECTIVE 2000/31/EC.

75 Recital 58 of The DIRECTIVE 2000/31/EC.

position in international fora[76]. Article 1(2) lists the topics necessary for realising the objective of Article 1(1). Articles 3-19 address these topics, e.g. the internal market in Article 3, commercial communications in Articles 6-8, Electronic Contracts in Articles 9-11,and code of conducts in Article 16.[77]

5.4.2. Legality of Electronic Contracts

The provisions of Articles 9-11 on Electronic Contracts complement the Directive 1999/93/EC on electronic signatures.

5.4.2.1. Treatment of Contracts

The formation of online contracts is an essential element of Electronic Commerce. Therefore, Article 9(1) determines that Member States have the duty to ensure that their legal system permits contracts to be concluded by electronic means. that legal requirements may not create obstacles for the use of electronic contracts, and that legal effectiveness and validity may not be deprived on the account of contacts being electronic. Formal requirements to be examined concern for example the medium used (paper, hand-written) or the presence of both parties.[78]Pursuant to Article 9 member states must allow contracts to be concluded by the electronic means. These contracts should be afforded the same validity and legal effect as contracts concluded in the conventional manner provides. This requirement demands legislative amendments, particularly in Germany.[79]

Article 9 gives the German legislator opportunity to clarify the legal validity of digital signatures. In particular, it is address the issue of the digital signature can replace a personal signature in cases where a written form is required pursuant to Section 126 of the German Civil Code (which requires that the document must be signed).[80]

---

76 Recital 59 of The DIRECTIVE 2000/31/EC.

77 Arno R. Lodder, "Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market", *available at: hattp//:*www.SSRNhttpssrn.comabstract=1009945(last visited on May 17, 2013).

78 *Ibid.*

79 "The Impact of the European E-commerce Directive", a*vailable at: hattp//:*www. internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe #applicable (last visited on May 18, 2013).

80 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at:*

Member states can provide for certain exceptions to the application of Article 9(1). These include:

- real estate transactions;
- contracts that involve a notary, public authorities or professions exercising public authority;
- contracts of suretyship;
- contracts concerning collateral; and
- contracts governed by family law or the law of succession.

5.4.2.2. The Information Requirements

Article 10 provides that a provider should provide clear and comprehensive information on its web site with respect to individual technical steps that must be followed to conclude the contract before its an order is placed. Details on the following issues should be provided:[81]

- Whether the service provider will file the concluded contract and whether it will be accessible;
- The technical means for identifying and correcting input errors prior to placing the order; and
- The languages in which the contract may be concluded.

Member states require to ensure that service provider indicates any relevant codes of conduct to which it subscribes. Finally, the contract terms and general conditions should be made available in a way that allows recipient to store as well as reproduce them. Article 10 does not apply to contracts concluded entirely through the e-mail.

5.4.2.3. Placing The Order

The Article 11 contained detailed regulations to conclusion of the contracts. According to the European Commission, the original proposal deals only with the case of provider making the contractual offer. But, the old version of Article 11, the provider had to confirm receipt of customer's acceptance of the contractual offer. The

---

*hattp//:*www.columbia.edu~mr2651ecommerce31stStatutesElectronicCommerceDirective.pdf (last visited on June 20, 2013).

81 "The Impact of the European E-commerce Directive", a*vailable at: hattp//:*www. internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe #applicable (last visited on May 18, 2013).

customer then had also to acknowledge receipt of that confirmation.[82]This provision was complicated and problematic in the countries where the web site only represents an invitation to negotiate. In such cases, the offer is made by customer. According to German law, it is the provider's confirmation of receipt proposed by European Commission which would comprise the acceptance of the customer's offer. It is doubtful to what extent a directive can amend applicable civil law provisions in the member state.[83]

5.4.3. Liability of Intermediary Service Providers

the Article 15 of the Directive says that member states may not impose the general obligation on the service providers to monitor information. Furthermore, the provisions in Articles 12-14 comprise a liability privilege. If the service provider can not satisfy conditions for restriction of its liability, it shall be liable in order to the applicable domestic legislation.[84]

5.4.3.1. Conduit

The Article 12 contains a service provider merely transmits information which is provided by the recipient of a service or provides access to a communication network is not liable for information transmitted if:

- it does not initiate the transmission;
- it does not select the receiver of the transmission; and
- it does not select or modify the information transmitted.

This provision read with Section 5(3) of the German Teleservices Act, according to which the person who only provides access for use, can is not liable for the third-party contents.[85] The Article 12 states that automatic, intermediate and transient storage of the information transmitted is also covered under the provision.

5.4.3.2. Caching

---

82 *Ibid.*

83 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu~mr2651 ecommerce31st StatutesElectronicCommerce Directive.pdf (last visited on June 20, 2013).

84 "The Impact of the European E-commerce Directive", a*vailable at: hattp//:*www. internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe #applicable (last visited on May 18, 2013).

85 *Ibid.*

'Caching' is the storage of data to increase the capacity and speed of the digital networks. The Data is stored temporarily in an operator's system to accelerate access by subsequent users. The service provider is not responsible for automatic, temporary storage and intermediate if:

- it does not modify the information;
- it complies with conditions on access to the information; and
- it complies with rules regarding to updating the information, which are recognized by and used within the industry. [86]

According to Article 13(1) the service provider must act swiftly to remove or block access to information which has stored upon obtaining actual knowledge of the fact that the information at initial source of the transmission which has been removed from the network or access to it has been blocked, or that a court or an administrative authority has ordered this.

5.4.3.3.Hosting

According to Article 14, a host provider is not responsible for the information stored if it has no actual knowledge that contents are illegal as well as acts swiftly to remove or block access to information upon becoming aware of illegality.[87]

However, problems arise when claimss made for damages, it is sufficient that there be an awareness of facts or circumstances that make illegality of an activity or information obvious. This opens way to civil law liability in cases of negligence.[88]

5.4.4. Codes of Conduct

The Commission and Member States shall encourage; (a) the drawing up of codes of conduct at Community level, by trade, professional. Consumer associations or organisations, which is designed to contribute to proper implementation of Articles 5 to 15, (b) voluntary transmission of draft the codes of conduct at the national or Community level to the Commission, (c) the communication to the Commission and Member States by trade, professional and consumer associations or organisations, of their assessment of application of their codes of the conduct and their impact upon the practices, habits or customs relating to the Electronic Commerce, (d) the accessibility

---

86 *Ibid.*
87 *Ibid.*
88 *Ibid.*

of these the codes of conduct in Community languages by electronic means, (e) drawing up of codes of the conduct regarding the protection of minors and human dignity.[89] The Member States and the Commission shall encourage involvement of associations or organisations representing consumers in drafting and implementation of codes of the conduct affecting their interests and drawn up as per paragraph 1(a). Where appropriate associations representing the visually impaired and disabled should be consulted.[90]

5.4.5. Out-of-Court Dispute Settlement

In order to the disagreement between the information society service provider and the recipient of the service, Member States shall ensure that, their legislation does not hamper the use of out-of-court schemes which is available under national law for dispute settlement which includes appropriate the electronic means. Member States shall encourage bodies responsible for the out-of-court settlement of consumer disputes to operate in the way that provides adequate procedural guarantees for parties concerned. Member States shall encourage bodies responsible for the out-of-court dispute settlement to inform the Commission of important decisions.[91] Member States shall ensure that the court actions available under the national law concerning information society services activities allow for fast adoption of measures designed to terminate any alleged infringement and to prevent any further impairment of interests involved.[92]

The legislation of the Member States may not hamper the use of alternative dispute resolution (hereinafter referred to as ADR) in case of a dispute between the provider and the recipient. Moreover, legislation should also allow online ADR. There exist already quite some ODR-sites, as yet mainly American. The Directive should be an impulse for the development of European ODR-sites.[93] Because ADR is meant to save money and time, and resolve conflicts without too much technical legal discussion being necessary, consumers probably benefit most from ADR. The

---

89 See, Article 16 of The Directive 2000/31/EC.

90 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu~mr2651ecommerce31st StatutesElectronicCommerceDirective.pdf (last visited on June 20, 2013).

91 See, Article 17 of Directive 2000/31/EC.

92 See, Article 18 of Directive 2000/31/EC.

93 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu~mr2651 ecommerce31st StatutesElectronicCommerceDirective.pdf (last visited on June 20, 2013).

settlement of in particular consumer disputes is encouraged in Article 17(2). At this moment an Extra Judicial Network of the EU is under development, as well a particular financial counterpart: FINNET.[94] The Commission eagerly wants to follow the developments regarding ADR and ODR. Therefore, they encourage those bodies responsible for out-of-court dispute settlements inform the Commission about their services, and about their practices, usages or customs relating to Electronic Commerce.[95]

5.4.6. Cooperation

Member States shall have adequate means for the supervision and investigation to implement this Directive effectively. It shall ensure that service providers supply them with the requisite information. Member States shall cooperate with other Member States; they shall appoint one or several contact points, whose details they shall communicate to other Member States and to the Commission. Member States shall provide the assistance and information requested by other Member States or by the Commission, including by appropriate electronic means. Member States shall make contact points which shall be accessible at least by the electronic means and from which the recipients and the service providers may (a) obtain the general information on contractual rights and obligations as well as on complaint and redress mechanisms available in event of the disputes, including practical aspects involved in use of such mechanisms, (b) obtain the details of authorities, associations or organisations from which they may obtain further information or practical assistance.[96] Member States shall encourage communication to the Commission of any significant administrative or judicial decisions taken in their territory pertaining to disputes concerning to information society services and practices, usages and customs relating to Electronic Commerce. The Commission shall communicate these decisions to the other Member States.[97]

5.5. The Uniform Electronic Transactions Act, 1999

---

94 *Ibid.*

95 Arno R. Lodder, "Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market", *available at: hattp*www.SSRNhttpssrn.comabstract=1009945(last visited on May 17, 2013).

96 See. Article 19 of The Directive 2000/31/EC.

97 Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu~mr2651ecommerce31st Statutes ElectronicCommerceDirective.pdf (last visited on June 20, 2013).

Recently, the internet has fastly removed geographic barriers and revolutionized the way world communicates and transacts business. In response to move towards a more paperless society, the Georgia Legislature passed the Uniform Electronic Transactions Act, 1999(hereinafter referred to as UETA). During the drafting process, the Drafting Committee incorporated much of the Model Law as well as some other American legislation, and was also mindful of complementary and possibly contradictory provisions of the American Uniform Commercial Code(hereinafter referred to as UCC).[98] Georgia is the 47th state to adopt the Act, which will take effect on July 1, 2009. The Act has established guidance and the uniform standards for the enforceability of the electronic transactions. The Act is voluntary and does not require parties to conduct business electronically. Parties must intend to conduct the transactions electronically. In those instances, the Act sets the following ground rules for the E-Commerce transactions:[99]

The scope of the Act is broad "Except as otherwise provided … this Act applies to the electronic records and the electronic signatures that relate to any transaction." This broad swath is subject to the limitations in the following three categories: the American Uniform Commercial Code (UCC) will independently cover the electronic transactions; wills and trusts, as these documents have the tradition of solemnity that paper conveys; and the third catchall category of those areas of the law for which individual state chooses to require paper-based transactions. The purpose of the Uniform Electronic Transactions Act, 1999 (hereinafter referred to as UETA) is to create legal recognition of the electronic records, electronic signatures. The Electronic Contracts: "the fundamental premise of this Act: namely, that the medium in which a record, signature, or contract is created, presented or retained does not affect its legal significance." Because the substantive law governing the underlying transaction may require the non-electronic records or signatures, the UETA achieves the purposes by overriding the substantive law on these requirements. For this reason, "a record or signature may not be denied legal effect or enforceability solely because it is in

---

98 Henry D. Gabriel, "The New United States Uniform Electronic Transactions Act : Substantive Provisions, Drafting History and Comparison to The UNCITRAL Model Law on Electronic Commerce", *available at: hattp//:*www.unidroit.orgenglish publicationsreviewarticles 2000-4-gabriel-e.pdf (last visited on May 18, 2012).

99 Esq.William J. Piercy, Esq. Kristin N. Zielmanski, "Georgia Adopts The Uniform Electronic Transactions Act", *available at: hattp//:*www.bfvlaw.comwp-contentuploads 201210piercy_ georgia-electronic-transactions.pdf (last visited on March 18, 2012).

electronic form," nor can a contract "be denied the legal effect or validity simply because the electronic record was used in the formation of the contract."[100]

Thus, if a law requires a record to be in writing or requires a signature, these requirements can be met by the electronic records or the electronic signatures. Another important issue is attribution – i.e., when and under what circumstances an electronic record or electronic signature is attributable to an individual. The UETA responds that if the electronic record or signature resulted from the person's action, then the record or signature will be attributed to that person. The act by a person may be proved in any manner, including a showing of any security procedure that was applied and to determine the identity of the person to which the electronic record or signature was attributable.[101]

There are also specialized rules governing contract formation by automated transactions. First, the contract can be formed by interaction of the electronic agents of the parties even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms or agreements. Second, a contract can be formed as the result of the interaction of an electronic agent and an individual, who is acting on his own behalf or on behalf of another individual, including by an interaction in which the individual performs actions that it is free to refuse to perform and which it knows or has reason to know will cause the electronic agent to complete the transaction or performance. Therefore, the Act provides that contracts can be formed by machines. The requisite intent necessary for the formation of a contract arises from the use and programming of the machine.[102]

5.5.1. Significance

This Act does apply to transactions under Articles 2 and 2A. There is every reason to validate the electronic contracting in these situations because the Sale and lease transactions do not implicate broad the systems beyond the parties to underlying

---

100 Henry D. Gabriel, "The New United States Uniform Electronic Transactions Act : Substantive Provisions, Drafting History and Comparison to The UNCITRAL Model Law on Electronic Commerce", *available at: hattp//:*www.unidroit.orgenglish publications reviewarticles 2000-4-gabriel-e.pdf (last visited on May 18, 2012).

101 Henry D. Gabriel, "The New United States Uniform Electronic Transactions Act: Substantive Provisions, Drafting History and Comparison to The UNCITRAL Model Law on Electronic Commerce", *available at: hattp//:*www..unidroit.orgenglish publicationsreviewarticles 2000-4-gabriel-e.pdf (last visited on May 18, 2012).

102 *Ibid.*

transaction. Further, sales and leases do not have so far reaching effect on the rights of third parties beyond the contracting parties. Finally, the area of sales, licenses and leases is that the Electronic Commerce is occurring to its greatest extent today. In the event, Articles 2 and 2A are revised as well as adopted in the future, the Uniform Electronic Transactions Act, 1999 (hereinafter referred to as UETA) will only apply to the extent provided in those Acts.[103]An electronic record/signature can be used for purposes of either more than one legal requirement, or may be covered by more than one law.

5.5.2. Utility of Electronic Records, Electronic Signatures and Variation by Agreement

Under the Act, a record or signature shall not be denied enforceability simply because it is in the electronic form. Despite of the electronic records and signatures have the same the legal effect as their paper and parchment ancestors. The party seeking to rely on the electronic record or signature must have an evidentiary foundation just as with a paper equivalent. [104]

Several situations in which the law requires that a party sign a document to be bound by it. The electronic signature will satisfy that requirement. The Act allows a notary public to notarize signature of another electronically. An electronic signature may be an electronic sound, symbol, or process. This may include the digitized image of the traditional ink signature, the typed name, the click through on the dialogue box, biometric measurements, or the encrypted authentication system and to constitute the electronic signature, the sound, symbol or process must be attached to a record and executed or adopted by a person intent to sign the record. The intent of electronic signature can be proven by any means, including surrounding circumstances or the efficacy of an agreed-upon the security procedure. The party seeking to enforce the signature lies on him the burden of proof.[105]

---

[103] Uniform Electronic Transactions Act (1999) : Drafted by The National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All The States at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23–30, 1999)., *available at: hattp//:*www www.yozons. comlinkeddocsueta.pdf (last visited on May 18, 2012).

[104] Esq.William J. Piercy, Esq. Kristin N. Zielmanski, "Georgia Adopts The Uniform Electronic Transactions Act", *available at: hattp//:*www.bfvlaw.comwp-contentuploads 201210piercy_ georgia-electronic-transactions.pdf (last visited on March 18, 2012).

[105] See, Sec 5 of The Uniform Electronic Transactions Act (1999).

The fundamental principle is in subsection (a) and elaborated by subsections (b) and (c), which require an intention to the conduct transactions electronically and preserve the right of a party to refuse to use the electronics in any subsequent transaction. The paradigm of this Act is two willing the parties doing transactions electronically. Therefore, it is appropriate that the Act is voluntary and preserves the greatest possible party autonomy to refuse the electronic transactions. Party agreement be found from all the surrounding circumstances which is a limitation on the scope of this Act. If this Act is to facilitate the electronic transactions, it must be applicable under circumstances not rising to the full fledged contract to use electronics. While absolute certainty can be accomplished by obtaining an explicit contract before relying on the electronic transactions. Despite of such a requirement would itself be an unreasonable barrier to Electronic Commerce, at odds with fundamental purpose of this Act. The requisite agreement must be determined from all available circumstances and evidence. [106]

5.5.3. Legal Applicability of The Act

The Act expressly recognizes that the contracts can be formed between the electronic agents even without human interaction. Where two computers are programmed with the parameters that may cause them to institute certain the transactions automatically, the enforceable contract may be formed between them. For example, if Automaker and Supplier do business through Electronic Data Interchange, Automaker's computer, upon receiving the information within certain pre-programmed parameters, will send an electronic order to the Supplier's computer. If the order falls pre-programmed parameters in Supplier's computer and Supplier's computer confirms the order and processes the shipment, this fully automated transaction which would constitute a binding contract under the Act.[107]

The retention of records solely in the electronic format is generally sufficient to satisfy a record retention requirement imposed by the law. Furthermore the

---

[106] Uniform Electronic Transactions Act (1999) : Drafted by The National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All The States at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23–30, 1999)., *available at: hattp//:*www www.yozons.comlinkeddocsueta.pdf (last visited on May 18, 2012).

[107] Esq.William J. Piercy, Esq. Kristin N. Zielmanski, "Georgia Adopts The Uniform Electronic Transactions Act", *available at: hattp//:*www.bfvlaw.comwp-contentuploads 201210piercy_ georgia-electronic-transactions.pdf (last visited on March 18, 2012).

maintenance of the electronic records may be outsourced as well as need not be physically maintained by person or entity charged retaining the records. The two primary requirements are that the records (1) must be accurate and (2) remain accessible for later reference. Remaining accessible requires that the electronic records must be converted to new formats if evolution of technology would render the records inaccessible otherwise.[108]

5.5.4. Legal Validity and Recognition of Electronic Records, Electronic Signatures and Electronic Contracts

While oral contracts are generally enforceable (albeit difficult to prove), there are certain situations as well as subject matters for which the law requires a written document. The Act confirms that an electronic record satisfies this 'writing' requirement. To constitute a 'writing' under the Act, an electronic record must be capable of retention by recipient atthe time of receipt. The electronic record is not capable of retention if sender or its information processing system inhibits ability of recipient to print or store the electronic record.[109] This section establishes the fundamental premise of this Act that the medium in which a signature, record, or contract is created, retained or presented does not affect it's legal significance. Hence, subsections (a) and (b) are designed to eliminate single element of the medium as a reason to refuse effect or enforceability to a record, signature, or contract.[110]

The fact that the information is set forth in an electronic, as opposed to paper, record is irrelevant. Subsections (c) and (d) provide positive assertion that the electronic records and signatures satisfy the legal requirements for writings and signatures. This provisions are limited to requirements in laws that the record be in writing or be signed. This section does not address requirements that imposed by other law in addition to the requirements for writings as well as signatures Subsections (c) and (d) are particularized applications of subsection (a). The purpose is to validate and effectuate the electronic records and signatures as equivalent of

---

108 *Ibid.*

109 Esq.William J. Piercy, Esq. Kristin N. Zielmanski, "Georgia Adopts The Uniform Electronic Transactions Act", *available at: hattp//:*www.bfvlaw.comwp-contentuploads 201210piercy_ georgia-electronic-transactions.pdf (last visited on March 18, 2012).

110 Uniform Electronic Transactions Act (1999) : Drafted by The National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All The States at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23–30, 1999)., *available at: hattp//:*www www.yozons. comlinkeddocsueta.pdf (last visited on May 18, 2012).

writings, subject to all of rules applicable to efficacy of a writing, except other rules which are modified by more specific provisions of this Act.[111]

5.5.5. Attribution and Effect of the Electronic Record and Electronic Signature

Under section 9 (a), as long as an electronic signature or electronic record resulted from a person's action, it shall be attributed to that person as the legal effect of that attribution is addressed in subsection (b). This section does not change existing rules of law pertaining attribution. The section assures that such rules will be applied in the electronic environment. The person's actions taken by human agents of the person, and actions taken by the electronic agent, i.e., the tool of a person.[112] this section does not affects the use of a signature as a device for attributing a record to the person. In fact, a signature is the primary method for attributing a record to a person. In the foregoing examples, once the electronic signature is attributed to the person, the electronic record would also be attributed to the person, unless the person established the fraud, forgery, or other invalidating cause. Therefore, a signature is not the only method for attribution.[113]

This section does determine the effect of a 'click-through' transaction. A 'click-through' transaction involves a process which, if executed with intent to 'sign,' will be an electronic signature. In the context of an anonymous 'click-through,' issues of proof will be paramount. This section may be relevant to establish that resulting the electronic record is attributable to a particular person whose the requisite proof, including security procedures, which may track the source of the click-through.

Once, it is proved that a record or signature is attributable to a particular party, the effect of the record or signature must be determined in the context and surrounding circumstances. The informing the effect of any attribution will be other legal requirements considered in light of context. Subsection (b) addresses effect of the record or signature once attributed to a person.[114]

5.5.6. Originality of Electronic Records

---

111 *Ibid.*

112 Uniform Electronic Transactions Act (1999) : Drafted by The National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All The States at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23–30, 1999)., *available at: hattp//:*www.yozons.comlinkeddocsueta.pdf (last visited on May 18, 2012).

113 *Ibid*.

114 *Ibid.*

The concept of the original document is problematic in an electronic medium. For example, as one drafts a document on a computer the 'original' is either on a disc or hard drive to which the document has been initially saved. If one periodically saves the draft, the fact is that at times the document can be first saved to the disc then to hard drive and at others vice versa. In such a case the 'original' may change from the information on the disc to the information on the hard drive. Indeed, it may be argued that the 'original' exists solely in Random Access Memory andthe original is destroyed when a 'copy' is saved to a disc or to the hard drive. In the event, in the context of record retention, the concern focuses on the integrity of the information, and not with its 'originality.[115]

This section allows parties to convert original written records to electronic records for retention as long as requirements of subsection (a) are satisfied. In the absence of the specific requirements to retain written records, written records may be destroyed once saved as the electronic records satisfying the requirements of this section. The subsection refers to information contained in the electronic record as a matter of clarity that critical aspect in retention is information itself. If the addressing and pathway the information regarding an e-mail is relevant, then that information should also be retained. Forthermore, if it is the substance of the e-mail that is relevant, only that information need be retained. Wise record retention would include all such information since what information will be relevant at a later time that will not be known.

5.5.7. The Time and Place of Sending and Receipt of the Data Message

Subsection (a) establishes rules to determine when an electronic record is sent. The effect of sending and its import are to be determined by other law once, it is determined that a sending has occurred. In order to have a proper sending, subsection requires that information be properly addressed or otherwise directed to recipient. According to this section, there must be specific information which will direct the record to the intended recipient. Although, the mass electronic sending is not precluded, a general broadcast message, sent to systems rather than individuals which would not suffice as a sending. The record will be considered sent once it leaves the control of sender, or comes under the control of recipient. The Records sent through

[115] See, Sec 12 of The Uniform Electronic Transactions Act (1999).

e-mail or the internet will pass through several different server systems. Accordingly, the critical the element when more than one system is involved is loss of control by the sender.[116]

However, the structure of number of message delivery systems is such that electronic records can actually never leave control of the sender. This section does not address effect of an electronic record that is thereafter pulled back, e.g., removed from a mailbox. The analog in the paper world should be removing a letter from a person's mailbox. Section 8 provides information electronically and the recipient's ability to receive the message should be assesed from the perspective of whether sender has done any action which could preclude retrieval. This is the case in regard to sending, since the sender must direct record to a system designated or used by the recipient.[117]

It is the paper analog to the recipient who never reads a mail notice. Subsection (f) states legal certainty regarding effect of the electronic acknowledgment and it only addresses fact of receipt, not the quality of content, nor whether the electronic record was read or 'opened.' Subsection (g) limits the parties' ability to vary the method for the sending and receipt that is provided in subsections (a) and (b) when there is the legal requirement for the sending or receipt. It is to noted that in other circumstances where legal requirements derive from other substantive law, to the extent that other law permits variation by agreement, this Act does not impose any other additional requirements and provisions of this Act may be varied to the extent provided in other law.

5.5.8. Transferable Records of Data Message

Section 16 is only an exception to the thrust of this Act to simply validate electronic media used in commercial transactions. Section 16 provides a means for expanding the Electronic Commerce. It provides certainty to lenders and investors regarding the enforceability of a new class of financial services. It is to be noted that legal protections afforded by Section 16 will engender development of the technological and the business models which will permit realization of the significant cost savings and efficiencies available through the electronic transacting in financial services industry. Although, only a bridge to more detailed consideration of the broad issues regarding to negotiability in an electronic context, Section 16 provides impetus

116 *Ibid.*
117 *Ibid.*

for that broader consideration while allowing continuation of developing technological and business models.[118]

5.5.9. Interoperability of Data Message

Sections 17-19 have been given as optional provisions to be considered for adoption by each State. Among the barriers to the Electronic Commerce are barriers which exist in the use of electronic media by state governmental agencies, whether among themselves or in external dealing with private sector. In the circumstances when the government acts as the commercial party, e.g., in the areas of procurement, the general validation provisions of the Act will apply. The government must agree to conduct transactions electronically with vendors and customers of government services.[119]Section 19 requires governmental agencies or state officers to take account of consistency in applications as well as interoperability to extent practicable when promulgating standards. This section is critical in addressing the concern that inconsistent applications can promote barriers greater than currently exist. Without these direction the myriad systems which could develop independently would be new barriers to the Electronic Commerce, not a removal of barriers. The key to interoperability is flexibility and adaptability. The requirement of the single system may be as big a barrier as the proliferation of many disparate systems.[120]

5.6. Indian Legislation: Information Technology Act, 2000

The Information Technology Act has been passed by the Indian Parliament with an object to facilitate E-Commerce, e-governance and to prevent Cyber Crimes. This legislation is unique in many respects. It provides legal recognition for the transactions carried out by means of the electronic data interchange and other means of electronic communication. It mandates electronic governance and provides infrastructure to achieve that goal. It chalks out an ambitious plan for preventing Cyber Crimes. It contains provision for the appointments of an Adjudicating Officer who shall be an expert in information technology to monitor any contravention and provides for the establishment of Cyber Appellate Tribunal. [121]It has, however, to be borne in mind that the Information Technology Act, 2000 (hereinafter referred to as

---

118 *Ibid.*
119 *Ibid.*
120 *Ibid.*
121 Farooq Ahmad, *Cyber Law in India* p.viii (New Era Law Publication, 4th edn., 2013).

IT Act, 2000) is not a separate code for electronic transactions but it is gap filler. It addresses the gray areas spawned by the internet but does not provide a separate legal regime for Electronic Commerce. The parent Act still governs the electronic transactions and where any legal requirement impedes electronic communication that has been removed by the IT Act, 2000. In doing so many existing principles have been either modified or altogether changed.[122]

The IT Act, 2000 has a limited scope. It does not cover all the issues, which have cropped up by the introduction of internet. While going through various provisions of the IT Act, 2000, it appears that many provisions lack harmony and it is quite possible that practical difficulties in applying these provisions will ensue in the near future. The machinery to prevent Cyber Crimes is not well equipped. The Cyber Appellate Tribunal is a one-man Commission, having law degree an essential qualification. Whereas Information Technology involves highly complex technical issues beyond the comprehension of an ordinary person who does not possess understanding of this technology[123]

The electronic transactions like other parts of the globe are in vogue in India. However, they were without legal security before the enactment of IT. Act, 2000.[124] The increasing growth of Electronic Commerce, popularly called E-Commerce, made it necessary to have legal protection to such transaction. The Indian Parliament took a step of seminal importance by passing the Information Technology Act, 2000.[125]This Act has three objects that are:

- To respond and give effect to the United Nations call to all States to give favourable consideration to Model Law when they enact or revise their laws so as to facilitate harmonization of the laws governing alternatives to paper based methods of communication and storage of information.
- To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly called as Electronic Commerce which involves the use of alternatives to paper based methods of communication and storage of information.

---

122 *Ibid.*

123 *Ibid.*

124 This fact was admitted by the Parliamentary Affairs Minister Shri Pramod Majahan in Parliament. See, *Hindustan Times*, May 16, 2000.

125 Hereinafter referred to as the IT Act, 2000.

- To facilitate electronic filing of documents with the Government agencies so as to promote efficient delivery of the Government services by means of reliable electronic records.

The Indian Parliament being alive to the ground realities such as lack of infrastructure for new technology, computer literacy and functional equivalents decided to limit the scope of the IT Act, 2000 and did not extend it to

(a) the negotiable instrument other than a cheque as defined in Section 13 of the Negotiable Instruments Act, 1881. The provisions of this Act, for the time being in force, shall apply to or in relation to, the electronic cheques and the truncated cheques subject to such modifications and amendments as -may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 by the Central Government in consultation with the Reserve Bank of India, by notification in the official Gazette.[126]

(b) A power of Attorney as defined in Section 1A of the Powers of Attorney Act, 1882;

(c) A trust as defined in Section 3 of the Indian Trusts Act, 1882;

(d) A will as defined in clause 4 of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by -whatever name called;

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;

(f) Any such class of the documents or transactions as may be notified by the Central Government in the official Gazette.[127]

The above documents include disposition of real estate that is commonly required to be in writing almost throughout the Common Law world. These exceptions will not present any impediment to the growth of Electronic Commerce. The functional equivalents will, with the passage of time, emerge in this area as well and even at present, there are clear hints in this direction. For example, Model Law

---

[126] See, Sec. 81-A of The Information Technology Act, 2000.

[127] See Sec. 1(4) of The Information Technology Act, 2000, This section reads : Nothing in this Act shall apply to documents or transactions specified in the First Schedule. This provision corresponds with Sec. 4(1) of The Singapore Electronic Transactions Act, 1988.

specifically deals with the bill of lading, electronic transfer of payment and the pseudonymous electronic cheque.[128]

The Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) extends to the whole of India, including the State of Jammu and Kashmir and has come into force on 17.10.2000. The provisions of the IT Act, 2000 shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.[129] It also applies to any offence or contravention committed outside India by any person irrespective of his nationality if that act or contravention involves a computer, computer system or computer network located in India.[130] The extra-territorial ambit of the IT Act, 2000 is not unusual. The provision giving extra-territorial jurisdiction is found in IT specific legislations of other jurisdictions also. Apparently, the need for such provision is driven by the borderless nature of the internet. These provisions are, however, viable only if there is mutual co-operation amongst enforcement authorities and Governments. The Indian IT Act, 2000 is unique in many respects. It casts its net very wide. It brings many issues under one umbrella for which separate legislations have been enacted in other jurisdictions. [131]

The Information Technology Act, 2000 (hereinafter referred to as IT Act, 2000) includes within its ambit legal recognition of the electronic records and digital signatures, authentication and retention of electronic records. It accords legal recognition to records, files or documents that are retained in an electronic form. It enables public institutions and government departments to issue electronic licences and permits and thus paves the way for electronic governance. It establishes the legal framework that will provide for the setting up of a public key infrastructure. The liability of the service providers for third party content has been clarified. The provisions for the appointment, powers and functions of the Controller of Certifying Authorities and the duties of the subscriber have been provided. This Act also makes offences like tampering with computer source document, hacking and publication of obscene information punishable. A provision for the establishment of special tribunal-Cyber Regulations Appellate Tribunal has also been made.[132]

---

128 Farooq Ahmad, *Cyber Law in India* p.29 (New Era Law Publication, 4th edn., 2013).
129 See, Sec.81 of The Information Technology Act, 2000.
130 See, Sec. 1(2) and 75 of The Information Technology Act, 2000.
131 Farooq Ahmad, *Cyber Law in India* p.30 (New Era Law Publication, 4th edn., 2013).
132 *Ibid.*

Conclusion

The UNCITRAL Model Law on theElectronic Commerce was adopted in 1996 with the purpose to help States in the information legislation with respect to the electronic communications and to serve as a reference aid for interpretation of existing international conventions and other instruments to avoid impediments to the Electronic Commerce. According to Article 1, the law applies to any sort of information in the form of data message which is used in the context of commercial activities but allows exceptions to be made by individual countries. Articles 6 and 7 are intended to focus on the fulfilment of traditional functions of writing because data messages can satisfy the traditional functions and therefore are 'functionally equivalent'. It recognizes future developments and applications which are unforeseeable because mere definition of the terms will be either too broad to comprehend or too narrow to develop new applications. The use of functionally equivalent language, this leaves the Model Law requirements broad enough to allow for new technologies and applications because this general 'framework' approach is more conducive to broad the international acceptance than a detailed the regime of mandatory rules.

The Model Law on E-Commerce has influenced many States regarding legislative drafting and proposals. Some Recent enactments and uniform laws now applicable in Canada and the US were influenced by the Model Law and the drafting committees from the two countries were exchanging ideas on the subjects. In the European Union, the Electronic Commerce Directive as well as the Electronic Signatures Directive were also influenced heavily by the Model Law and Draft Rules. In addition, drafting committees for the implementation of these proposed laws seemed to be substantially influenced by each other's work to reduce diverging interpretations.

This is a product of different legal systems as well as a tendency toward comprehensive, detailed law reform in EU nations contrasted by the less hands on approach in the US. In the global perspective, there is the same problem, whether UNCITRAL is known as Model Law and Electronic Fund Transfer Act in US but still they fail to make any appropriate law which can regulate the transaction and solve the

dispute and problems which generally occurs in E- commerce. Therefore, there is a need of present time to draft new laws which must have effective role in regulating the E-Commerce in national as well as global perspective.

Issues relating to E-Commerce have been started to be tackled at the international level either in inter-governmental circles or in other foras. This is the case relating to intellectual property issues in the context of the World Intellectual Property Organization (WIPO), which is about extend to new fields like the internet domain names issues, through WIPO's prerogatives in area of trademarks for example. Nowadays, the issue of domain names has been fascinating in terms of how existing structures (such as WIPO) and new ones (like ICANN) will adapt to a rapidly changing environment. In that respect, WIPO has done well, and showed its ability to address new issues and challenges without renouncing any of its initial mandates or responsibilities. It is to be noted that other inter-governmental bodies may find inspiration in example of WIPO to upgrade and update their own approaches to ecommerce related issues.

The main economic issues raised by E-Commerce for the World Trade Organization and developing countries is that Lack of appropriate physical infrastructure has so far placed major restraints on the growth of E-Commerce in developing countries . It is felt to advocate three policy prescriptions. First, all things considered, it will be most appropriate to classify the E-Commerce as trade in services with The General Agreement on Trade in Services (GATS) discipline applied to it. since this matter is still under negotiation, developing countries should be make sure that the E-Commerce should not classified as goods trade with zero custom duty pact made permanent. Such an outcome would liberalise all E-Commerce by default, undermining their bargaining power. Second, presently, there is some disagreement about whether an international internet transaction is to be classified as cross-border trade or consumption abroad. Therefore, it makes some sense to classify international internet trade as cross-border trade.

The directive of the German legislature faced new challenges that should be resolved within 18 months from the date on which it became effective. It was taken as an opportunity to clarify the legal validity of digital signatures. It was considered that Requirements of the production of evidence and the distribution of the burden of proof must also be developed. In addition, the directive suggested to Germany to

harmonize its competition law because the provider could be subject to the national law according to the country-of-origin principle. Hence many providers regarded this as an opportunity to circumvent Germany's strict rules of fair trading by establishing themselves in a different member state. For this reason, some started demanding the abolition of the Act on Discounts and the Ordinance on Bonuses, both of which are somewhat incomprehensible to the foreigners. The legislature should regulate the admissibility of advertising by e-mail, which should have already been regulated in accordance with the Directive on Distance Sales 97/7/EC. Furthermore, the E-Commerce Directive by stating in Article 10(2) that means of individual communication other than the voicemail systems and fax may be used only where there is no clear objection from the consumer. In this regard, the E-Commerce Directive considered that the e-mail must be identified as an advertisement in the header, and that providers must regularly consult the Robinson lists. These conditions provide recipients to delete these e-mails without opening them and also provide the opportunity to prevent the sending of such communications. It is to be seen what extent the country-of-origin principle will be applied by German judges following its implementation in national law. It is also unclear how the courts, especially in summary proceedings, are to assess the legal situation according to foreign law.

The Uniform Electronic Transactions Act does not attempt to or succeeds in setting out all the legal rules that are necessary to effectuate Electronic Commerce. The Act try to achieve that is a legal mechanism to allow Electronic Commerce to develop further while more specialized rules can be developed and adopted in specific areas of commerce. It is certain that the future will quickly bring us domestic and international laws governing the electronic sale and securitization of goods, electronic negotiable instruments, documents of title and letters of credit. Each of these areas already has legal coverage for electronic transactions. However, until the law with these specialized areas of commercial practice, the UETA provides commercial practices in the United States to continue to grow in the electronic medium.

The Information Technology Act, 2000 is a commendable piece of legislation for India and is a bold step, which has taken in the right direction. It upholds the spirit of the UNCITRAL Model law. However, it should be cleared in mind that the Model law is not intended to cover every aspect of the use of Electronic Commerce. Hence, there has been left other substantive areas that need to be addressed like consumer

protection, data protection, spamming, intellectual property, etc. It may be advised to have separate legislation for some of the above rather than complicating the Information Technology Act, 2000 with numerous things. Similarly, although the provision relating to electronic signatures suited the country's prevailing circumstances and available technology at the time of the legislation, it should be amended with course of time in order to accommodate changing technological advances. E-Commerce has potential to generate wealth for developing countries and present legislation is to facilitate E-Commerce transactions is merely a first step. There is need to give greater attention to promoting electronic governance. The Information Technology Act of India is finest work of the Government of India and it can hope that it may be an inspiration for other developing countries to legislate E-Commerce laws as envisaged by the United Nations Resolution on the UNCITRAL Model law. Furthermore, these countries will have the advantage of observing and learning from India's experience and taking measures to address some more issues at the enactment stage itself.

CONCLUSION AND SUGGESTIONS

Conclusions

The information technology is the most recent development in the history of mankind. In the beginning, our economy was agrarian in nature, then became industrial and now is in the process of becoming knowledge or information based economy. These fast developments of information and communication technologies have brought changes in the way of communication, which has revolutionised business practices.

Consequently, the business transactions are being conducted electronically because it can be accessed on computer connected to internet situated in any place of the world. E-Commerce means traditional way of conducting business with the help of electronically means. E-Commerce is the buying and selling products by World Wide Web or internet. The E-Commerce is one of the most important developments of the international trade, which provides several advantages along with serious legal challenges. With the fast expansion of internet in the 21st century, E-Commerce provides the new opportunities that are accessible to both large corporations as well as small corporation. But, there is also need to provide adequate legal framework for E-Commerce so that national and international trade may expand their horizons and their basic rights like privacy, intellectual property, and prevention of fraud, consumer protection etc are all taken care of. E-Commerce is a new way of conducting, managing and executing business transactions using computer and telecommunication networks but E-Commerce is supposed to improve the productivity and competition by providing unprecedented access to an on-line global market place with millions of customers and thousands of products and services. Electronic commerce services are very easy, flexible, and speedy to use. It is, therefore, accepted throughout the world and become international character.

Furthermore, E-Commerce cannot flourish in an uncertain legal environment. Therefore, Legal principles should not only be formulated but also properly implemented in India. There are many benefits by using E-Commerce such as it is cheap, easy and fast. It can provide enhanced services by incorporating E-Commerce. The individuals can save time, search costs and can avail best offers/discounts associated with purchase of products/services online buying/selling. It can be

concluded that E-Commerce is beneficial to both buyer and seller as win-win situation. There are some shortcomings but it may be removed by improvements in technology to make E-Commerce easy, convenient and secure.

The E-Commerce is categorised as business-to-business, business to consumer, consumer-to- business, consumer-to-consumer, non–business and Government and Inter-organizational transactions. It has examined various combinations of tools including legal and business process and policies, but security technology is very crucial to success E-Commerce in India. E-security would give credibility to E-Commerce against online frauds and hacking etc. which can be achieved by adequate legal framework and a protective technology. Thus, the technology of cryptography provided legal sanction by The Information Technology Act, 2000 would go a long way boosting E-Commerce.

The security of electronic record has become major issue in electronic commerce, which has been attempted to solve by passing legislation. The essential feature of a secure electronic record is that it cannot be changed in the process of storage because a secure electronic signature will sign it. The law recognizes electronic counterparts of paper documents and signature, which is admissible in the court of law. Judge has to be careful while dealing with the integrity of data because electronic record may be tempered and there is no foolproof way of authentication. The electronic commerce system is operated over open network a system that is outside of geographical boundaries of the nation. The Researcher has attempted to solve moot questions concerning the applicability of the state laws to transactions that may be initiated by a consumer in one state who uses a financial institution headquarter in another state to payments to recipients located in other states by means of a computer at some unknown location. These challenges are beyond the nation whereas The Information Technology Act, 2000 deals with the domestic legal issues. Hence, there is a need of International Corporation regarding E-Commerce implementation globally.

The Information Technology Act, 2000 is a commendable piece of legislation for India and it holds the basic spirit of UNCITRAL Modal law. This Act was the need of the time as a cyber specific legislation on E-Commerce for smooth and proper governance of the new technology. The new environment demanded new set of laws because the internet is being used for pornography, gambling, trafficking in human

organs and prohibited drug, hacking, infringing copyrights and violating individual privacy etc. It is, therefore, needed for a law to regulate the activities in cyber space to fill the gap specially relating to regulation of E-Commerce in cyber space.

The Information Technology Act, 2000 has specified and defined not only provision relating to E-Commerce but also computer crime and offences along with punishment resulting amendment in the Indian penal code. The Information Technology Act, 2000 covers several issues relating to cyber world than Model law. The Information Technology Act, 2000 is welcomed but there is still some grey area that should properly be addressed. The Information Technology Act, 2000 addresses mainly three areas that make possible E-Commerce transaction, e-governance and curb cyber crime by regulating the internet. Hence, it is to be noted that Model law is not intended to cover every aspect of the use of electronic commerce. Therefore, many grey areas, which are needed to be addressed properly by Information Technology Act, 2000 such as Consumer Protection, Data Protection, Spamming, Intellectual Property, Domain Name Dispute, Electronic Payment System, Privacy and E-Taxation. It is considered that there should be separate legislation for some of the matter above mentioned rather than making complicated The Information Technology Act, 2000 with numerous things.

The Information Technology Act, 2000 has introduced the concept of Attribution, Originator, and Acknowledgement and Time & Place of Dispatch. The wisdom of the Act is that it involves government machinery to investigate the contravention of the Act and appoint controller of certifying authorities for the purpose of this act. It is to be noted that controller can exercise supervision over the certifying authorities, specify the form and content of a digital signature corticated, and facilitate the establishment of any electronic system by certifying authority. The controller has power to grant a licence to issue digital signature certificate, renewal of licence, rejection of licence and suspension of licence. The certifying authority has power to issue the digital signature certificate in the prescribed form.

Similarly, every subscriber is under legal obligation to see all representation made by him to the certifying authority and all material relevant to the information contained in the digital signature certificate is true. The Information Technology Act, 2000 has provisions for the establishment of cyber Appellate Tribunal to hear appeals of the aggrieved person of an order made by the controller of adjudicating officer.

The tribunal has its own procedure to regulate its affairs rather than follow other procedural laws. However, cyber appellate tribunal shall have to be guided by the principles of natural justice. Hence, it can be said that The Information Technology Act, 2000 is really a brave effort to promote and regulate a secured electronic environment except certain grey area that is to be addressed yet.

India is first among a few countries, which has passed its separate law regarding E-Commerce, and other Information Technology enabled services. Although, The Information Technology Act, 2000 is quite comprehensive and well defined, there is still various areas connected with information technology that has been left uncovered in The Information Technology Act, 2000. However, the credit goes to legislative competence to frame such Act on new environment. It is really an appreciated act to bring forth legislation on E-Commerce in tune with the needs of Indian state and society. Moreover, it is open for amendment according to the exigencies of the situation and needs of the society.

The section relating to liability of network service providers which has been revised to limit the liability of the intermediaries to cases where they are either active participate or have failed to exercise the due diligence. Thus, it is proposed to make rules regarding such intermediaries because such provision will encourage the service providers to invest in providing network and other infrastructure facilities.

The Information Technology Act, 2000 has succeeded to foster a digital environment in which the advantages of new technologies are being tapped by effectively facilitated electronic commercial transaction, electronic filing maintenance of electronic records and electronic government transactions. The Information Technology Act, 2000 has adopted functional equivalents approach in which a proper legal framework is to be evolved to validate and authorize the use of electronic data interchange, electronic records and electronic signatures. Hence, this Act also deals with issues of privacy, contraventions relating to electronic transaction and information offences to regulate an information and technology regime. Thus, it may be said that the Information Technology Act has addressed to a considerable extent the legal questions involved in adopting the cyber medium for communication of contract and commerce.

The electronic contract or online contract is the backbone of the E-Commerce, which has been thoroughly studied. E-Contract is a contract that is in a digital form. The contract formation issues have been moot issues, which arise at time when one purchases goods or services online. There is not much clarity as to what constitutes consideration, how to determine the intention of parties as well as capacity of parties to enter into an electronic contract together with validity of digital signature. If all the essential ingredients of the E-Contract are present in the contract, E-Contract is valid and enforceable before court of law. It is to be noted, once all requirement of the law are fulfilled by E-Contract then contract provides multifarious opportunities to E–business. It is, therefore, said that E-Contract is the key to the future of E-Commerce. The E-Contracts have two major problematic issues that are speed and automation because there is hardly any chance to rectify error in E-Contract's communication, as a result, the certainty and predictability of remedies available in tangible contract has become complicated by electronic measures. Thus, there is need to adopt international legal framework to establish the same certainty and predictability for E-Contract as compared to paper contract.

The Information Technology Act, 2000 has been passed by Indian legislation taking inspiration from Model law that gives legal recognition of electronic records and electronic signature which are functional equivalent of paper based documents and handwritten signature. The electronic signature provides authenticity, confidentiality and non–reproduction of the electronic data but electronic signature cannot help to determine the exact time of dispatch or receipt of the electronic records. Moreover, the date spoofing technique may be used to change the date of receipt or dispatch of electronic records in all those servers through which electronic record would travel. Due to this technique, it would be difficult to determine the exact time of formation of the E-Contract. The solution of this problem is to make mandatory time stamping service with electronic signatures.

Several kind of E-Contract has thoroughly been analysed that is click–wrap, shrink-wrap, E-mail contract and Electronic Data Interchange contract. There are many legal issues, which arise relating to E-Contract, which cannot be answered by the Indian Contract Act, 1872. There is need to either amend contract act or bring new legislation to deal with such issues. Hence, The Information Technology Act, 2000 has been passed but it is not a complete Code for regulating E-Contract because the

Indian Contract Act, 1872 is still fundamental law for formation of contract. Although the Amendment Act, 2008 has brought many changes in The Information Technology Act, 2000 and Section 10 A of The Information Technology Act, 2000 has been inserted to regulate E-Contract in the term of communication of proposal, acceptance and its revocation. There is still need to provide certainty pertaining to determining time of formation of E-Contract. However, there are still grey areas, which have to be analysed yet. It may be submitted that if the provisions of Indian Contract Act, 1872 are inconsistent with the provision of the Information Technology Act, 2000 or where express provisions have been mentioned by the Information Technology Act, 2000, then the only The Information Technology Act, 2000 should prevail and apply.

The evidentiary value of electronic records is very important to make electronic record admissible in the court of law and it is based on the quality and integrity of electronic data. Consequently, Indian Evidence Act, 1872 deals with the evidentiary value of the electronic records under Section 3 of the Indian Evidence Act, 1872 as evidence means and includes all document including electronic document produced for the inspection of the court and such documents are called documentary evidence. Hence, it may be concluded that documentary evidence includes electronic records and it stands at par with conventional form of documents.

Substantiating the discussion, it may be said that E-Contract is quite similar as other hard copy contract either in terms of essential ingredient of contract or its evidentiary value. All E-Contracts are legally valid contracts and enforceable as they are legalized by The Information Technology (Amendment Act 2008) Act, 2000 and one could be made liable for any infringement with the terms and conditions.

The Intellectual Property Right in fast developing digital world has become most complicated areas of cyber law because the Information Technology Act, 2000 does not mention word pertaining to copyright, trademarks and patents. Thus, technological developments impose serious challenges to the basic principles of Intellectual Property laws such as Distribution, Caching, Protection of Confidential Information, Patents, Copyrights, Trademark and Domain Names, Liability for Defamatory Statements over Networks, Content Liability and Protection, Payment Mechanism for Internet Commerce, Money Laundering, Taxation Issues, Prohibition and Regulated Activities etc. Some changes have been made by amendment in Intellectual Property laws to fill the gap, which arises due to the technological

advancement, but there is still need to make major amendments to deal with the challenges posed by the internet and electronic revolution. Hence, India has passed this legislation on E-Commerce that the Information Technology Act, 2000, which enables transactions signed electronically to be enforceable in a court of law. The Information Technology Act, 2000, does not deal trademark rights over domain name owners. The trademark act is not efficiently equipped to deal with web-related issues. Hence, the adequate law is required to deal with such important issues.

Undoubtedly, the rapid growth of internet has provided unprecedented new opportunities to cyber crime offenders and this development poses serious challenge to the present law and criminal system because the kind of cybercrime which does not exist in physical world but do exist in cyber world, which span the globe through the instantaneous communication of internet, and provides new opportunities to offenders for anonymity, deception and disguise the emergence of cybercrime that imposes moot questions for criminologist. The theories of crime were based on assumption of territorial world but the cyberspace is radically different from the terrestrial world. In this way, criminology itself is challenged to adopt perspectives to grip with cyber crime or to develop new concepts and vocabularies, which would be fit with online digital world.

The cybercrime relating to E-Commerce, one fundamental aspect was found that creates serious difficulties relating to jurisdiction because the nature of internet is such that the geographical and political boundaries have become irrelevant in relation with the digital world. In this way, it can be said that a person's access to a computer and the internet may be participated, attempted or a planned criminal act from anywhere in the world. The internet is considered as analogous the high seas. It is advised that the cybercrime should be tried under the international crimes on the same pattern as offence of piracy under the law of sea, which may be tried in any country.

The common form of internet related crime has introduced wide range of fraudulent activities that are perpetrated by using internet such as e-mail, websites and auction houses. It is very difficult to identify criminals who are using false or stolen identities. It is to be noted that the move from the terrestrial to virtual environment provides many advantages to fraudsters. However, technique has been explored to respond cyber fraud but it is not simple tool, technique or policy that can curtail fraudulent online activities. The crime does not concern with frontier because

criminals do not have the sense of patriotism, humanism or jurisprudence. Nevertheless, now days, the crimes of the modern age, being borderless need law to be international character. It may be said that globalization is good but it emerges as challenge to the criminal justice system. Similarly, India, being the information superpower, has passed Information Technology Act, 2000 in cyber law to address the emerging challenges of the information society but still so little has been done and so much is yet to be done in this regard.

Therefore, cyber crime is a new form of crime that has emerged due to the computerization of various activities. With the rapid growth of information technology, cyber crimes are increasing with the increase of internet connectivity. To deal with the problem, Information Technology Act, 2000 provides penalty for the offences relating to internet. A tribunal named Cyber Appellate Tribunal has also been established to provide speedy solutions. So, it may be conjectured that every possible care is taken by the Information Technology Act, 2000 to cope with the problems but there are still many situations, which are either not dealt properly or not covered under Information Technology Act, 2000. Hence, there is need to frame well equipped national or international legal regulation pertaining to cybercrime

Universal cyberspace jurisdiction means any state whose people are affected by an electronic activity that state shall have jurisdiction to adjudicate matter and the decision will be enforced by the international convention of enforcement of foreign courts. Personal cyberspace jurisdiction is based on the local accessibility resulted local effects upon people since websites target the whole cyberspace territory being accessed by all jurisdiction. The internet is a place where people meet to communicate and businesses meet consumers and sell their products. Hence, the nature of cyber world is very vast and it is the ability of others to access, use, and communicate with the computer, which gives value to the network. It is the time to consider a cyberspace jurisdiction relating to cyberspace actions, which is not feasible effect on real world, but it can be felt only in cyberspace. It is, therefore, advised that there should be Cyber Courts and Cyber Arbitral Tribunals to have jurisdiction to solve all actions taking place on the internet and decisions and awards should be made according to International Conventions on recognition and enforcement of Foreign Awards as well as E-Awards. Thus, these Courts and Arbitral Tribunals should be considered equal and independent forms of dispute resolutions.

The traditional method to ascertain jurisdiction has become irrelevant in cyberspace from the perspective of the enforcement of rules and regulations and from the traditional understanding of territorially separate jurisdiction. The nature of the Internet is such that it is not possible to determine a particular Internet Protocol address to be situated on a given day because it is very easy to change the physical location of the webpage (from server to server). It makes difficult to regulate the Internet activity because of territorial restrictions. Hence, the global computer network is destroying the link between geographical location and the power of government to control over online activities, the effects of online behaviour on individuals and the ability of physical location to give notice of which sets of rules to apply. Consequently, the traditional jurisdictional norms cannot be applied on the Internet and will not have effect in redressing any dispute.

In the United State, the courts have extra territorial jurisdiction over dispute when the defendant fulfils condition of long-arm jurisdiction of the courts in which the suit is instituted. In India, the court assumes jurisdiction over defendant on the basis of cause of action relating to computers and the internet. The principle, on which the decision of the court of both countries is based, is quite similar because the concept of cause of action adopted in India is broad enough to allow an Indian court to have jurisdiction over matter of dispute even when a small part of the cause of action arose within Indian Territory. On the other hand, the parties to contract may select an agreed forum or choice of law as a part of their agreement with each other in order to smoothen matters at trial. Thus, a forum between two conflicting laws chooses to apply its own law. The fact is that the nature of internet need separate jurisprudence relating to adjudication of the matter of cyberspace. The statement relating to jurisdiction as proposed by United State and European courts and other international organisations are only guide to determine jurisdiction of courts relating to the internet. Thus, the issue of jurisdiction applicable law and enforcement of the judgment are not confined to only national boundaries. Jurisdictional problem on internet has become global in nature, hence, requires global solution.

UNCITRAL has adopted The Model Law on Electronic Commerce in 1996 with objective to help States drafting their legislation with respect to electronic communications and to aid for the interpretation of existing international conventions as well as other instruments to avoid impediments to electronic commerce. The Model

Law provides that the law should be applied to any kind of information in the form of electronic data message used in the context of commercial activities whereas it allows exceptions to be made by individual countries. UNCITRAL has determined that data messages can satisfy all the traditional functions because it recognizes future developments and applications are unforeseeable. The Model Law on E-Commerce has become modal which has influenced several States to draft legislation relating to E-Commerce. The Recent uniform laws on E-Commerce have been passed by Canada and the United State were influenced by the Model Law, and drafting committees from the two countries are exchanging ideas on the subjects. It is to be noted that the Model Law and Draft Rules have influenced the Electronic Commerce Directive and the Electronic Signatures Directive greatly. Thus, several other issues pertaining to E-Commerce, which have been started to be tackled at the international level in either inter-governmental or other foras. Similarly, World Intellectual Property Organization (WIPO) has started to extend new issue of Internet domain names through WIPO's prerogatives in the field of trademarks.

The Development of E-Commerce and new technologies requires regulatory adjustment pertaining to privacy, authentication, legal validation of electronic contracting, security of transactions, liability and the jurisdiction applicable on the transaction and also consumer protection. Although, not all issues may be addressed through the international rule making mechanisms, yet some of the issues can be addressed by such international mechanism. Moreover, it is difficult to establish jurisdiction for the application of tax law because it is just impossible to ascertain the location from where internet services are being accessed due to multiple locations of modems, server and routing equipment. It is to be noted that it requires paying attention on the functioning of the network infrastructure to sell and distribute product on internet. The merchants who rely on the Internet for the distribution of their products are complaining for the poor facility of network system. Hence, Public policies are needed to monitor the access to, and supply of digital product.

The Uniform Electronic Transactions Act provides a legal mechanism to allow electronic commerce, which is still in its initial stage, need further development to promote E-Commerce in a well-planned manner. It is therefore needed to develop specialized rules and adopt in specific areas of commerce. Therefore, it should be domestic and international laws on the subject of the electronic sale of goods,

electronic negotiable instruments, documents of titles and letters of credit. Thus, The Uniform Electronic Transactions Act (UETA) is capable to regulate E-Commerce practices in the United States to grow in the electronic medium.

German legislature adopted the directive on E-Commerce is known as directive on Electronic Commerce. It provided an opportunity to clarify the legal validity of digital signatures. It had to develop requirements relating to the production and the distribution of the burden of proof. The directive is dealt with the contract concluded online while ordering party could access the confirmation of receipt on its mail. The E-Commerce Directive provides that the e-mail must be identified as an advertisement in the header and that providers have to consult the Robinson lists. In this way, recipients can not only delete these e-mails but also prevent to send such communications. As the provider is the subject to national law as per the country-of-origin principle, other providers take this opportunity to circumvent Germany's rules of fair trading by establishing themselves in a different member state.

These are the main economic issues raised by E-Commerce for the World Trade Organisation (WTO) and developing countries. It is most suitable to classify E-Commerce as trade in services with General Agreement on Trade in Services (GATS) discipline applied to it. However, developing countries do not want that E-Commerce should be classified as goods trade with zero custom duty which would be result of liberalised all E-Commerce by default. It would go against their national interest. There is disagreement on the issue of international Internet transactions to be classified as cross-border trade or consumption abroad. Hence, all legal issues of electronic commerce cannot be regulated by national or international law because the parties to electronic transactions are permitted to agree among themselves on certain rules and standards which is applicable on their contractual relationships in most jurisdiction.

The Information Technology Act is a laudable legislation enacted by Indian government. and it would be an inspiration for other developing countries to legislate E-Commerce laws. These countries may have the advantage of observing and learning from India’s experience and taking measures to address some other issues at the enactment of their law on E-Commerce. In global perspective, there is quite similar problem being faced throughout the world, whether United Nation Convention International Trade Law (UNCITRAL) or Electronic Fund Transfer Act (EFTA) in

United State. There is not any appropriate law to regulate such transaction and solve the dispute, which occurs in E-commerce. Therefore, there is a great need to make effective and adequate law to regulate the E-Commerce in National and global perspective.

Suggestions

In order to grasp the developing opportunities in E-Commerce in India creatively and productively, the vibrant and didactic suggestions may be put forward by the researcher to make techno-legal development more effective and functional -

1. The Information Technology Act, 2000 is comprehensive but there are still many issues of E-Commerce which is silent (e.g. Intellectual Property Right, Domain Name Dispute, Electronic Payment System, Data Protection, Protection of Consumer Rights, and E-Taxation). It is, therefore, advised to pass a specific separate legislation on regulation of E-Commerce keeping in mind all remaining issues on which The Information Technology Act, 2000 is silent.
2. The Digital Signature or Electronic Signature ensures authenticity, confidentiality and non-production of the electronic record but the electronic signature cannot help to know exact time of dispatch or receipt of the electronic record. Moreover, the date spoofing technique can be used to change the date of receipt or dispatch of electronic record in all servers according to their convenience. It is, therefore, advised to make mandatory the use of time stamping service along with electronic signature.
3. At present, the regulation of E-Commerce has become an important topic not only in India but also in rest of the world. To achieve desire result of new legal challenges, the adequate legal mechanism has to be evolved, developed and appropriate restriction should be imposed to safeguard the individual interest as well as national interest.
4. To curb the Cybercrime and Crime related to E-Commerce, there should be established special Cyber Tribunal and Cyber Court, Online International Dispute Settlement Mechanism as well as International Tribunal Enforcement of Decision and Foreign Award.

5. The info-structure is required for E-Commerce promotion rather than the hardware and physical infrastructure.
6. Internet access to enterprise is not enough to realize the potential of E-Commerce to compete effectively in the global market but the digital environment needs other factor to be placed.
7. India should ask the World Trade Organization to assist in studying the global implications of E-Commerce from the developing country angle whereby India can remove the shortcomings which is being done in regulation of E-Commerce effectively.
8. The initiatives for a strategic approach to protect E-Commerce should be a dynamic rather than static approach.
9. An effective policy and regulatory environment should be created to help in the development of E-Commerce and harmonized national approaches.
10. So far as taxation in E-Commerce is concerned , there should be adopted future tax policy on E-Commerce to compete with the traditional commerce on a level playing field consist with the principle of international taxation and with simple rules to follow.
11. The issue of cyber jurisdiction has become of global character which cannot be genuinely addressed by passing only national legislations. Therefore, cyber jurisdictional issue requires global solution. Hence, an international treaty relating to uniform rules applicable to E-Commerce is badly needed to be adopted.
12. Although, The Information Technology Act, 2000 has been passed but it does not form a complete code for E-contract. The Indian Contract Act, 1872 is still fundamental law for contract formation which causes problem in respect with cyber space because in the formation of E-contract, there are many issue which cannot be answered within exiting provision of Indian Contract Act. It is, therefore, required to either amend the Indian Contract Act, 1872 or bring a new legislation specifically dealing with the E-Contract.
13. Some issue relating to E-Contract should be more clarified in order to facilitate basic principle for the time of formation of E-contract.
14. The principle of Attribution in the formation of E-Contract should be provided more strengthen by using identification technology.

15. The government does not give due attention to new peril resulting slow legislation to respond emerging new legal issues and problems concerning to E-Commerce and E-Contract. It is, therefore, advised that before making law, information technology's experts, researchers and practitioner should have been consulted in the specialized field of law.

16. The application of information technology is a constant developmental process. Therefore, the vibrant and effective legal regulatory mechanism should be developed at required pace.

17. The limited Scope of The Information Technology Act, 2000 should be extended to include such issues, which have been left uncovered by the present act such as Payment Mechanism, Intellectual Property Law, E-Taxation and Negotiable Instrument etc.

18. The Private International Law rules regarding jurisdiction should be adopted to resolve the problem to some extent in respect of forum of case, application of law and enforcement of jurisdictions in foreign countries.

19. Several existing doctrines have not remained relevant because of advent of the internet especially in the field of Intellectual Property Law which is needed redefinition. Hence, there is need

    19.1 To modify the doctrines according to the digital challenges which constrict the scope of the Copyright Act, 1957.

    19.2 To re-interpret the provision of the Copyright Act, 1957 in the light of digital environment.

    19.3 To amend the Copyright Act, 1957 to fill the gaps which have been created by the use of cyber space, the trademark over the internet and its protection is essential for the growth of the E-Commerce.

    19.4 To define the Trademarks Right of Domain Name Owners.

20. The Information Technology Act, 2000 has mentioned different layers of authorities, which require some more changes to bring positive changes in the present criminal legal system.

21. The Extradition Act, 1962 should be amended by inclusion of cybercrime like hacking and cyber terrorism which are transnational in nature and poses bigger threat to national security.

22. The unconventional cyber crimes, which involve wide use of information technology, should be also required to take adequate measures by the law enforcement agencies on top priority to curb such crime.

Summing up the discussion, it can be said that business conducting through E-Commerce is growing rapidly but national and international bodies are too slow to evolve solution of the challenges posed by E-Commerce because the existing tenets of income taxation based on rules has been outdated in context of present Indian scenario. Hence, there is an immediate need to evolve equitable tenets for cross-border E-Commerce transactions so that there may be equitable distribution of tax revenues among nations. India should adopt such measures as to become beneficiary of the E-Commerce revolution along with the United States. The Researcher has tried to the fundamentals of the E-Commerce, as it is a new phenomenon. It is E-Commerce that has brought the harmonization of trade practices between the developed and developing countries. E-Commerce has the potential to become the global medium for the conduct of commercial activities, which need technological advancements. In cyber disputes, the main litigants are regulatory agencies, personal computer companies, Internet Service Providers, individuals, firms and companies that have established a presence on the Internet. Cyber law is an area of law, which is an offshoot of commercial law in India and elsewhere. Thus, the internet is a goldmine but without adequate and effective legal protection, it may become a landmine. The effective management with legal documentation will go a long way for protecting E-Commerce.

The Information Technology Act, 2000 is a brilliant piece of legislation in order to facilitate internet trade and to provide alternative paper based method of communication and strong of information. Moreover, it provides and promotes delivery of government Services by means of reliable electronic records. Subsequently, according to the need of time, it has been amended in 2008 to remove legal gap. The Information Technology Act, 2000 was technology specific and speaks about a particular procedure for authentication of the electronic records. However, that procedure had its own certain limitation but amendment 2008 has changed the legal position of electronic signature in order to fine tune with the need of time. However, there is still need to make certain changes in other provisions so as to remove inconsistency in them. The Information Technology Act, 2000 is very

complex over the formation on electronic contract and over to elaborate mechanism for controlling certification authorities stand in appose to more minimalist approaches adopted in other jurisdictions.

The many issues arise by E-Commerce have to be resolved by judiciary. It is felt to reframe the existing doctrines, which were developed in real space, had been inapplicable in several situations in cyberspace because E-Contract reduces geographical barriers and enhance the possibility of consumers entering into transnational contracts. This creates issue of private international law, but legal regime on this matter is quite obscure. Moreover, there is no uniformity of the law relating the jurisdiction, recognition and enforcement and application of law. Hence, it can be said that jurisdictional issue has become international character and passing national laws. The issue is a global one and resolution must be adopted an international treaty relating to uniform rules applicable to E-Commerce, jurisdiction of the courts and enforcement of the judgments.

Thus, cyber crime refers to criminal activities taking place through computers and computer networks, knowingly or intentionally access and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer data base, computer, system, or computer network to devise or execute any unlawful scheme, or wrongfully control or obtain money, property or data. It concerns individuals, corporate bodies and institutions, which are instrumental for entry into cyberspace, provide access to cyberspace, create the hardware and software, which enable people to access cyberspace and use their own computers to go online and enter cyber space. Main litigants in cyber disputes are telephone service provider companies, providers, schools, colleges, universities and finally, those individuals, firms and companies that have established a presence on the internet. At present, cyber crime in India is alterations of data are hard realities. The computer requires physical protection and Additional safety measures needed for computer and the backup information preserved proves an invaluable guide in case of computer crime. Countries like United State of America, United Kingdom, Germany, Japan, France, and India have framed laws relating cyber crimes. Consultation of these works can go a long way to make better cyber laws to check cyber crime in India and all over the world.

BIBLIOGRAPHY

A. Acts, Statutes and Legislations

[1]. The Arms Act, 1959

[2]. The Banker's Book Evidence Act, 1891

[3]. The British Computer Misuse Act, 1993

[4]. The Central Excises and Salt Act, 1944

[5]. The Central Sales Tax Act, 1956

[6]. The Civil Procedure Code, 1908

[7]. The Companies Act, 2013

[8]. The Copyright (Amendment) Act,1999

[9]. The Copyright Act, 1957

[10]. The Code of Criminal Procedure, 1973

[11]. The Digital Millennium Copyright Act,1998

[12]. The Electronic Transactions Act, 1999

[13]. The Finance Act, 2003

[14]. The Florida Electronic Signature Act, 1996

[15]. The General Clauses Act, 1897

[16]. The Illinois Electronic Commerce Security act, 1998

[17]. The Immoral Traffic (Prevention) Act, 1956

[18]. The Income Tax Act, 1961

[19]. The Indecent Representation of Women (Prohibition) Act, 1986

[20]. The Indian Contract Act,1872

[21]. The Indian Copyright Act, 1957

[22]. The Indian Evidence Act, 1872

[23]. The Indian Evidence Act, 1872

[24]. The Indian Patent Amendment Act, 1999

[25]. The Indian Penal Code, 1860

[26]. The Indian Penal Code, 1860

[27]. The Indian Trade Mark Act,1999

[28]. The Information Technology (Certifying Authority) Regulations, 2001

[29]. The Information Technology (Certifying Authorities) Rules, 2000

[30]. The Information Technology Act, 2000

[31]. The Maine Criminal Code -Computer Crimes, 1989

[32]. The Malaysia Computer Crimes Act, 1997

[33]. The Malaysia Digital signature Act, 1997

[34]. The Malaysian Computer Crimes Legal Act, 1997

[35]. The Malaysian Electronic Signatures Act, 1997

[36]. The New Zealand Electronic Transactions Act, 2002

[37]. The Patent Cooperation Treaty, 1998

[38]. The Patents Act, 1970

[39]. The Reserve Bank of India Act, 1934

[40]. The Rome Convention, 1980

[41]. The Sale of Goods Act, 1930

[42]. The Singapore Electronic Transactions Act, 1998

[43]. The Texas Penal Code -Computer Crimes,1985

[44]. The Trade and Merchandise Marks Act, 1958

[45]. The Trade Related Aspect of International Property Rights (TRIPS)

[46]. The UCC Article 2B 1998

[47]. The UNICITRAL Model law on Electronic Commerce 1996

[48]. The Utah Digital Signatures Act, 1995

[49]. The WIPO Copyright Treaty, 1996

[50]. The WIPO Performance and Programme Treaty, 1996

B. Books, Discussion Papers, Policy Guides, Reports

[1]. Ahamad, Tabrez, *Cyber Law E-Commerce and M- Commerce* (A.P.H. Publishing Corporation, 1st ed., 2003).

[2]. Ahmad, Farooq, *Cyber law in India* (New Era Law Publication, 4th edn., 2013).

[3]. Bakshi, P.M., *The Constitution of India* (Universal Law Publishing Co. Pvt .Ltd. 8th edn.,2007).

[4]. Bidgoli, Hossein, *Electronic Commerce: Principles and Practice* (Academics, California, 2002)

[5]. Brenner, Susan W., *Cyber: Criminal Thereats from Cyberspace* (Pentagon Press, New Delhi. 1st edn., 2012).

[6]. Chaubey, R.K., *An Introduction to Cyber Crime and Cyber Law* (Kamal Law House, Kolkata, 1st edn., 2008).

[7]. Chris, Reed, John, Angel, *Computer Law* (Universal Law Publishing, Indian Reprint, 4th edn., 2002).

[8]. Chssick, M., Kelman, A., *Electronic commerce: law and practice*, (Thomson Professional Pub. Co, 2nd edn.2000).

[9]. Davidson, Alan, *The Law of Electronic Commerce* (Cambridge University Press, New York, 1st edn.,2009).

[10]. Diwan, Parag, Sharma, Sunil, *Electronic Commerce: A Manager Guide To E – Business*(Vanity Books International, New Delhi, 5th edn., 2009).

[11]. Dudeja, V.D., *Cyber Crimes and Law: Crimes in Cyber Space; Scams and Frauds* (Commonwealth Publishers, 1st edn., 2002).

[12]. Dudeja, V.D., *cyber crimes and law: cyber crimes and law enforcement* (Commonwealth, 1st edn., 2002).

[13]. Fatima, Talat, *Cybercrimes* (Eastern Book Company, Lucknow, 1st edn.,2011).

[14]. Gaur, K.D., *A Textbook on The Indian Penal Code* (Universal Law Publishing Co. Pvt. Ltd New Delhi, 4th edn., 2013).

[15]. Kamath, Nandan, *The Law Relating to Computers, Internet and E-Commerce* (Universal Law Publication Co.2nd edn., 2000).

[16]. Kaushik, Anjali, *Sailing Safe in Cyberspace* (SAGE Publication Ltd, London, 1st edn, 2013).

[17]. Kesari, U.P.D., *The Administrative Law* (Central Law Publications, 2003).

[18]. Kumar, Sujeet, *Encyclopaedia of Cyber Laws* ABD Publishers, New Delhi, 1st edn., 2011).

[19]. Malthan, Rahul, Law *Relating to Computers and Internet* (Butterworths India, New Delhi,1st edn., 2000).

[20]. Panagariya, Arvind, *E-Commerce, WTO and Developing Countries* (Blackwell Publishers Ltd, Oxford UK, 2000).

[21]. Radin, Margaret Jane, Rothchild, John A., et.al., *Internet Commerce: The Emerging Legal Framework* (University Casebook Series, Foundation Press, New York 2002) .

[22]. Roosenoer, Jonathan, *Cyber Law* (R.R. Donnelley and Sons, Harrison Burg, New York, 1997).

[23]. Sharma, Diwan, *Electronic Commerce: A Managers Guide to E-Business* (Vanity Books International,1st edn.,2000).

[24]. Sharma, Vakul, *Information Technology Law and Practice* (Universal Law Publication Co., 1st edn., 2004).

[25]. singh, Alwyn didar, *E-Commerce in India : Assessments and Strategies for The Developing World* (Butterworths, India1st 2008).

[26]. Singh, Yatindra, *Cyber Laws* (Universal Law Publishing Co., 2nd edn., 2005).

[27]. Smith, J.C., Hogan, B., *Criminal Law* (Butterworth and Company Publishers Ltd., London, 6th edn., 1988).

[28]. Stephenson, Peter, *Investigating Computer-Related Crime* (CRC Press, Washington, 2000).

[29]. Turner, J.W.C. , *Kenny's Outlines of Criminal Law* (University Press, Cambridge, 19th edn., 1966).

[30]. Verma, S.K. , Mittal, Raman (eds.), *Legal Dimensions of Cyberspace* (Indian Law Institute, New Delhi, 2004) .

[31]. wadhhra, B.L., *Intellectual Property Law Handbook* (Universal Law Publishing Co. Pvt. Ltd, 2nd edn., 2000)

[32]. Walden, Ian, *Computer Law* (Oxford University Press, 5th edn., 2003).

[33]. Yar, Majid, *Cyber Crime and Society* (SAGE Publications, London, 1st edn., 2006).

[34]. Zhao, Yun, *Dispute Resolution in Electronic Commerce* (Brill Academic Publishers, The Netherlands, 1st edn., 2005).

C. Articles and Papers

[1]. Abbasi, Behnam, "Intellectual Property: Legal Challenges and Opportunities in E-commerce Platform," 2(2) *Journal of Basic and Applied Scientific Research* (2012).

[2]. Abhilash, C. M., "E-Commerce Law in Developing Countries: An Indian Perspective" 11 (3) *Information & Communications Technology Law* (2002).

[3]. Ahmad Mir, Farooq, "Authentication of Electronic Records: Limitations of Indian LegalApproach" 7(3) *Journal of International Commercial Law and Technology* (2012).

[4]. Ahmad Mir, Farooq, "Emerging Legal Issues of E-Commerce in India" 2(2) *International Journal of Electronic Commerce Studies* (2011).

[5]. Ahmad, Farooq, "Electronic Commerce: An Indian Perspective" 9(2) International *Journal of Law and Information Technology* (2001).

[6]. Anand, Pravin, Barheer, Shamnad, et.al., “Internet and Intellectual Property Sights.” Chartered Secretary (August,2000).

[7]. Anil, Samtani, “Electronic Commerce in Asia: The Legal, Regulatory and Policy Issues” 9(2) *International Journal of Law and Information Technology* (2001).

[8]. Arora, Rajiv, Banwet, D.K., “E-Commerce Implementation in India: A Study of Selected Organizations” 10 (1) *Asia-Pacific Development Journal* (June, 2003).

[9]. Bansal, Rashmi, “Growth of the Electronic Commerce in China and India: A Comparative Study” 12(4) *Journal of Asia-Pacific Business* (2011).

[10]. Basu, Subhajit, Jones, Richard, “E-Commerce and The Law A Review of India's Information Technology Act, 2000” 12(1) *Contemporary South Asia* (March, 2003).

[11]. Basu, Subhajit, Jones, Richard, “Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000”, 17th BILETA Annual Conference April 5th - 6th, 2002 Free University, Amsterdam, *available at: http://* www.bileta.ac.uk /02papers/basu.html (last visited on October 11, 2012).

[12]. Baxi, Daksha, Shah, Bijal, “Electronic Commerce Taxation Evolves in India” *available at: http://*www.nishithdesai.comfileadminuser_uploadpdfsElectronic _Commerce _Taxation_evolves_in_India.pdf (last visited on February 22, 2012).

[13]. Biswas, Tushar Kumar, “Data and Information Theft in E-Commerce, Jurisdictional Challenges, Related Issues and Response of Indian Laws” 27 *Computer Law & Security Review* (2011).

[14]. Blythe, Stephen E., “Romanian E-Commerce: A Critical Analysis and Recommendations for Improvement,” 2(1) *International Journal Emerging Science* (March, 2012).

[15]. Castellani, Luca G., “The Role of UNCITRAL Texts in Promoting A Harmonized Legal Framework For Cross-Border Mobile Payments” 8(3) *Washington Journal of Law, Technology & Arts* (2013).

[16]. Christensen, Sharon, “Formation of Contracts by Email – Is it Just the Same as the Post?” 1(1) *Queensland University of Technology Law & Justice Journal* (2001).

[17]. “Computer and Internet Crimes", *available at: hattp//*:www.cyberspacelaw .com/ crimes.asp (last visited on May 8, 2012).

[18]. Dasgupta, Parikshit "India: Defining Jurisdictions in E-Commerce Taxations: Application of Traditional International Taxation Principles to E-Commerce",*available at* :*http://*www.mondaq.comindiax22619income+taxdefining+ jurisdictions+in+ecommerce+taxations (last visited on September 18, 2011).

[19]. Dasgupta, Parikshit, "India Defining Jurisdictions in E-commerce Taxations", *available* at: *http://* www.mondaq.comindiax22619Income+TaxDefining+ Jurisdictions +in+Ecommerce+Taxations (last visited on September 12, 2012).

[20]. Data, Subhashis, "E-Commerce: An Overview in The Indian Context",31(7-12) *Charted Secretary* (2001).

[21]. Davies, LJ., "A Model for Internet Regulation" (1998)., *available at: http://* www.scl.org. /content/commerce (last visited on October 12, 2013).

[22]. Desai Associates, Nishith, "Legal Issues in E-Commerce" *available at*: *http*://www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf (last visited on February 15, 2013).

[23]. dorn, James A., "The Future of Money in The Information Age," *available at*: *http://*www.cato.org/pubs/books/mpney(last visited on June 12, 2011).

[24]. Downing, Ricard E., "The Benefits and Obstacles of E-commerce: Toward an Understanding of Adoption" 5(2) *Journal of Internet Commerce* (2006).

[25]. Dubey, Arti, *Cyber Law and Terrorism* (National Conference on Cyber Laws and Legal Education, NALSAR University of Law, 2000).

[26]. E-Commerce: Issues for Developing Countries" *Economic and Political Weekly* (April 21, 2001).

[27]. Electronic Commerce and Work Programme in WTO" *available at: http://* commerce.nic.in /trade/international_trade_oi_ecommerce.asp (last visited on April 15, 2013).

[28]. Electronic Commerce Directive: Directive 2000/31/EC of The European Parliament and of The Council, *available at: hattp//:*www.columbia.edu ~mr2651ecommerce31stStatutes ElectronicCommerceDirective.pdf (last visited on June 20, 2013).

[29]. "Electronic Contracts-A Basic Understanding" *available at: http://*www. lexvidhi.com /article-details/electronic-contracts-a-basic-understanding -41.html (last visited on November 11, 2012).

[30]. Fangfei Wang, Faye, “Obstacles and Solutions to Internet Jurisdiction A Comparative Analysis of the EU and US laws” 3(4) *Journal of International Commercial Law and Technology* (2008).

[31]. Gabriel, Henry D., “The New United States Uniform Electronic Transactions Act : Substantive Provisions, Drafting History and Comparison to The Uncitral Model Law on Electronic Commerce” *available at: hattp//:*www. .unidroit. orgenglishpublications reviewarticles2000-4-gabriel-e.pdf (last visited on May 18, 2012).

[32]. Guidelines of E-Commerce: Ministry of International Trade and Industry (MITI), Japan (1996)., *available at*: *http://*www.kantei.go.jp/foreign/980817 densi.html (last visited on June 3, 2012).

[33]. Hampton, Jennifer M., "Experts to Probe Yahoo! Nazi Auctions" *E-Commerce Times*, (August 14, 2000)., *available at: http://*www.ecommercetimes. comlperllstory/4020.html. (last visited on March 25, 2012).

[34]. Impact of the European E-commerce Directive, *available at: hattp//:* www.internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe#applicable (last visited on May 18, 2013).

[35]. Intellectual Property in E-Commerce: Prepared for World Intellectual Property Organization's Worldwide Academy, by Franklin Pierce Law Center, *available at http://*www.uop.edu.jodownloadresearchmembersWIPO.pdf (last visited on May10, 2012).

[36]. Intellectual Property Issues Related to Electronic Commerce under World Intellectual Property Organization (WIPO), Small And Medium-Sized Enterprises Division Geneva Switzerland, *available at http:*//www. wipo.intexportsiteswwwsmeene_commercepdfip_ecommerce.pdf (last visited on March 19, 2011).

[37]. Ismail, Ihab A., Kamat, Vineet R., “Evaluation of Legal Risks For E-Commerce In Construction” *Journal of Professional Issues in Engineering Education And Practice* (October, 2006).

[38]. Jawahitha, Sarabdeen, “Cyberjurisdiction and Consumer Protection in E-Commerce” 21 *Computer Law & Security Report* (2005).

[39]. Jawahitha, Sarabdeen, Hamid, Noor Raihan Ab, “Electronic Contract and The Legal Environment”, *available at: http://* www.irfd.org/events/wf2003/ papers_global /R38.pdf (last visited on February 15, 2013).

[40]. Jobodwana, Z. Ntozintle, “E-Commerce and Mobile Commerce in South Africa: Regulatory Challenges” 4(4) *Journal of International Commercial Law and Technology* (2009).

[41]. Kannabiran, G., Narayan, P.C., “Deploying Internet Banking and Ecommerce-Case Study of A Private-Sector Bank in India” 11(4) *Information Technology for Development* (2005).

[42]. Kaur, Pradeep, Joshi, Mukesh M , “E-Commerce in India: A Review” 3(1) *International Journal of Computer Science and Technology* (January-March, 2012).

[43]. Kaur, Rajinder, Aggarwal, Rashmi, “Cyber-squatting: Legal implications and Judicial Approaches: An Indian Perspective” 27 *Computer Law & Security Review* (2011).

[44]. Kerimov, Nuran G., “Current Problems of International Taxation of Electronic Commerce”, *available at*: *http://*digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1023...stu... (last visited on October 12, 2014).

[45]. Khandelwal, Rishabh, “Understanding E –Contracts and Its Impacts”, *available at: http://*accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html (lastvisited on May 3, 2013).

[46]. Konoorayar, K Vishnu, “Regulating Cyberspace: The Emerging Problems and Challenges” *Cochin University Law Review* (2003).

[47]. Kshetri, Nir, “Barriers to E-Commerce and Competitive Business Models in developing Countries: A Case Study” 6 *Electronic Commerce Research and Applications* (2007).

[48]. Lal Bhasin, Madan, “E-Commerce Payment Systems” 4(1) *Chartered Secretary* 45(2007).

[49]. Lodder , Arno R., “Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in The Internal Market”, *available at: hattp//:*www. SSRN httpssrn.comabstract=1009945(last visited on May 17, 2013).

[50]. Mali, Adv Prashant, “E-contract: Now Admissible in Court” , *available at: http://* dqindia. ciol.com/ content/top_stories/2010/1010122701.asp(last visited on April 6, 2013).

[51]. Mancuso, Salvatore, “Consumer Protection in E-Commerce Transactions: A First Comparison between European Law and Islamic Law” 2 (1) *Journal of International Commercial Law and Technology* (2007).

[52]. Mann, D., Sutton, M., "Net Crime: More Change in the Organization of Thieving" 2 *British Journal of Criminology* (1998).

[53]. Martin, Charles H., “The Electronic Contracts Convention, The CISG, and New Sources of E-Commerce Law” 16(46) *Tulane Journal of International & Company Law* (2008).

[54]. Miller, Jim, “Answers to Frequently Asked Questions about Electronic Money or E-Money and Digiytal Cash”, *available at: http*:// www.ex.ac.ukRDavies /arian/ emoneyfaq.html (last visited on February 19 2012).

[55]. Mohammadi, Mohammad, “Challenges of Security in the Law of E-Commerce” 10(5) *Life Science Journal*(2013).

[56]. Mohanty, R.P., Seth, D., et.al., “Quality Dimensions of E-Commerce and their Implications”, 18(3) *Total Quality Management & Business Excellence* (2007).

[57]. Muenchinger, Nancy, “E-Commerce -US” 16 (6) *Computer Law & Security Report* (2000).

[58]. Nagpal, Rohas, “Ecommerce - Legal Issues”, *available at: http://*www. asianlaws. orglibrarycyber-lawselectronic-contracts.pdf (last visited on July 10, 2011).

[59]. Olsson, Henry, “Electronic Commerce and Intellectual Property Developments in Europe” 5 *Journal of Intellectual Property Rights* (2000).

[60]. “Online Contract and Its Validity”, *available at: http://* ashishlal.wordpress. com/2011/02/12/online-contract-in-context-of-internet/(last visited on September 15, 2013).

[61]. Phang, Andrew, Seng, Daniel, “The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code” 7(2) *International Journal of Law and Information Technology* (1999).

[62]. Polony, Joseph, “Computer Frauds Law Enforcement Response” 6(4) *FBI Bulletin* (May, 1998).

[63]. Primer on Electronic Commerce And Intellectual Property Issues, World Intellectual Property Organization (WIPO)., *available at http*//:www. ehealthstrategies.comfiles_primer.pdf (last visited on March 2, 2013).

[64]. Raina, Kapil, "Evidentiary Value of E-Contracts", *available at: http://*www. legalserviceindia.com/article/l127-E-Contracts.html (last visited on February 5, 2013).

[65]. Raipuria, Kalyan, "Electronic Commerce Opportunities for Indian Exports" *Economic and Political Weekly* (August 26-September 2, 2000).

[66]. Rao, Suneeti, "Information Technology Act Consumers' Perspective" *Economic and Political Weekly* (September 15, 2001).

[67]. Rastogi, Rajiv, " India: Country Report on E-Commerce Initiatives" Director Department of Information Technology: Ministry of Communication and Information Technology India, *available at*: *http://*www.unescap. orgtidpublicationpart_three2261_ind.pdf (last visited on February 2, 2011).

[68]. Rathore, Siya, "Electronic Contracts: Understanding Digital Goods and their Sale and Purchase", *available at: http://www*.expertscolumn.com /content/electronic-contracts-understanding-digital-goods-their-sale-and-purchase (last visited on November 10, 2012).

[69]. Rathore, Subhas P., Das, Bharat B., Cyber *Crimes: The Emerging Trends And Challenges* (National Conference on Cyber Laws and Legal Education, NALSAR University of Law 2001).

[70]. Rice, Dennis T., "Jurisdiction and E Commerce Disputes in United States and Europe" Presentation by Committee on Cyberspace Law and Business Law Section at the Annual Meeting of the California State Bar, Monterey (October 12, 2002).

[71]. Ricketson, Sam, "The Berne Convention for the Protection of Literacy and Artistic Works," *Center for Commercial Law Studies* (1987).

[72]. Rosner, Norel, "Features-International Jurisdiction in European Union E-Commerce Contracts", *available at*: *http://*www.llrx.com/features/eu_ecom.htm (last visited on November 8, 2010).

[73]. Rusch, Jonathan J., 'The Social Engineering of Internet Fraud," *available at: hattp//:*www.isoc.org/inet99/proceedings/3g/3g_2.htm (last visited on May 3, 2012).

[74]. Rustard, Micheal, Eisenschmidt, Lori E, "The Commercial Law of Internet Security" 10(2) *High Technology Law Journal* (1995).

[75]. Satapathy, C., "Legal Framework for E-Commerce" *Economic and Political Weekly* (July 18, 1998).

[76]. Satapathy, C., “Taxing Electronic Commerce” *Economic and Political Weekly* (May 9, 1998)

[77]. Satapathy, C., “WTO Work Programme on E-Commerce” *Economic and Political* (September 29, 2001).

[78]. Save, Peter, Deveaux, Sarah, "Jurisdiction in Cyberspace", IDG News Service. (Friday July 28, 2000)., *available at: http://*www.pcworld.comlnewsarticle. asp?aid= 17868. (last visited on March 25, 2012).

[79]. Savirimuthu, Joseph, “Online Contract Formation: Taking Technological Infrastructure Seriously,” 2 *University of Ottawa Law & Technology Journal* (2005).

[80]. Shah, Aashit, Nagree, Parveen, et.al., “Legal Issues in E-Commerce,*” available at: http://*www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf (last visited on January 6, 2012).

[81]. Sharma, B.R., Mehta, Runa, “Information Technology Act, 2000: An Answer to 21st Century Legal Squabbles” 38(1-4) *Civil &Military Law Journal* (2002).

[82]. Sharma, Kunal, Singh, Amarjeet, *et.al.,* “SMEs and Cybersecurity Threats in Ecommerce” 39 (5-6) *EDPACS: The EDP Audit, Control, and Security Newsletter* (2009).

[83]. Sharma, Shweta, Mittal, Sugandha, “Prospects of E-Commerce in India,” Haryana, India, *available at:http://*www.rimtengg.comiscetproceedingspdfsadv_ nw_ tech 43 .pdf (last visited on June 4, 2012).

[84]. Shaunakbali, “Analysis on The Concept of Jurisdiction”, *avalaible at hattp://*www.jurisonline.in(last visited on May 15, 2011)

[85]. Singh, Didar, “Electronic Commerce issues of Policy and Strategy for India”(2000)., *available at*: *http*://www.icrier.orgpdfwp-86.pdf(last visited on March 20, 2013).

[86]. Sudalaimuthu, S., Lilly, J, “Emerging Trend of E-Commerce in India”, *available on http://*www.fibre2fashion.comindustry-articlemarket-research-industry-reports emerging-trend-of-e-commerce-in-indiaemerging-trend-of-e-commerce-in-india1.asp(last visited on October 12, 2013).

[87]. Sushanth, S. Sai, “E-Commerce and Law: Trends and Challenges” 3(2) *UACEE International Journal of Advances in Computer Science and its Applications* (2013).

[88]. Tarafdara, Monideepa, Vaidyab, Sanjiv D., "Challenges in the adoption of E-Commerce technologies in India: The role of organizational factors" 26 *International Journal of Information Management* (2006).

[89]. Tasneem, F., "The Legal Issues of Electronic Contracts in Australia*"* 1(2) *International Journal Management Business Research* (2011).

[90]. Thatch, David, "Personal Jurisdiction and the World Wide Web: Bits (and Bytes) of Minimum Contacts" 23 *Rutgers Computer and Technology Law Journal* (1997).

[91]. The text of the UNCITRAL Model Law on Electronic Commerce, *available at http://*www.uncitral.org/cn-index.htm. (last visited on February 10, 2013).

[92]. Tubrazy, S. J., "E-contracts in Cyber Space", *available at: http://*www. articlesbase.com/cyber-law-articles/econtracts-in-cyber-space-502731.html (last visited on March 5, 2011).

[93]. "Understanding Electronic Contracts", *available at: http://*www.nalsarpro.org /CL/Modules/Module%201/Chapter3.pdf (last visited on June 5, 2013).

[94]. Uniform Electronic Transactions Act (1999): Drafted by The National Conference of Commissioners on Uniform State Laws and by it Approved and Recommended for Enactment in All The States at its Annual Conference Meeting in Its One-Hundred-And-Eighth Year in Denver, Colorado (July 23–30, 1999)., *available at: http//:* www.yozons.comlinkeddocsueta.pdf(last visited on May 18, 2012).

[95]. United Nations Conference on Trade and Development: Electronic: Commerce and Development, *available at: http://*www.unctad.orgenDocsposdtem11. en.pdft (last visited on April 5, 2013).

[96]. Vaithianathan, Sridhar, "A Review of E-Commerce Literature on India", *available at*: *http://*download.Springer.Comstaticpdf186art%253a10.1007%25 2fs10660-010-9046-0.Pdfauth66=1393853765_Ceb2a84f1fc05f57feba8b3b560 86344&Ext =.Pd (last visited on February 1, 2013).

[97]. Vittalachar, Ashwini, "Hurdles to Electronic Execution Of Commercial Contracts in India", *available at: http://*www.narasappa.com/resources/e-Contractsby AshwiniVittalachar.pdf (last visited on April 5, 2013).

[98]. While Paper on E-Commerce, OECD (1997)., *available at*: *www.oecd. org/sti/2093249.pdf* (last visited on June 7, 2012).

[99]. William J. Piercy, Esq., Kristin N. Zielmanski, Esq.,, " Georgia Adopts The Uniform Electronic Transactions Act" *available at: hattp//:*www.bfvlaw. comwp-contentuploads201210piercy_georgia-electronic-transactions.pdf (last visited on March 18, 2012).

[100]. Wittmann, Jeffery E. , BC., Vancouver, "Electronic Contracts" Negotiation and Drafting Major Business Agreements Conference Federated Press (October 2007) *available at: http://*www.wdwlaw.ca/ELECTRONIC_CONTRACTS_ 111007 _2803 12. pdf (last visited on April 5, 2013).

[101]. World Intellectual Property Organization (WIPO): Contribution to The World Summit on The Information Society (WSIS), Geneva,(February 17,2003).

[102]. Write B., Eggs in Basket, "Distributing the Risks of Electronic Signature",6 *Computers & Law* (1995).

[103]. Zainol, Z. A., "Electronic Data Interchange (EDI) and Formation of Contract: A Malaysian Perspective" 7(3) *International Journal of Law and Information Technology* (1999).

D. Journals

[1]. Aligarh Law Journal

[2]. Annual Survey of Indian Law

[3]. Asia-Pacific Development Journal

[4]. British Journal of Criminology

[5]. Center for Commercial Law Studies

[6]. Chartered Secretary

[7]. Civil &Military Law Journal

[8]. Civil and Military Law Journal

[9]. Cochin University Law Review

[10]. Computer Law & Security Report

[11]. Computer Law & Security Review

[12]. Computers & Law

[13]. Contemporary South Asia

[14]. E-Commerce Times

[15]. Economic and Political Weekly

[16]. Electronic Commerce Research and Applications

[17]. FBI Bulletin

[18]. High Technology Law Journal
[19]. Indian Bar Review
[20]. Information & Communications Technology Law
[21]. Information Technology for Development
[22]. International Journal Emerging Science
[23]. International Journal Management Business Research
[24]. International Journal of Computer Science and Technology
[25]. International Journal of Electronic Commerce Studies
[26]. International Journal of Information Management
[27]. International Journal of Law and Information Technology
[28]. Journal for Constitutional and Parliamentary Studies
[29]. Journal of Asia-Pacific Business
[30]. Journal of Basic and Applied Scientific Research
[31]. Journal of Indian Law Institute
[32]. Journal of Intellectual Property Rights
[33]. Journal of International Commercial Law and Technology
[34]. Journal of Internet Commerce
[35]. Journal of Professional Issues in Engineering Education And Practice
[36]. Life Science Journal
[37]. Queensland University of Technology Law & Justice Journal
[38]. Quest for Justice
[39]. Rutgers Computer and Technology Law Journal
[40]. Total Quality Management & Business Excellence
[41]. Tulane Journal of International & Company Law
[42]. UACEE International Journal of Advances in Computer Science and its Applications
[43]. University of Ottawa Law & Technology Journal
[44]. Washington Journal of Law, Technology & Arts

E. Supreme Court of India Documents

[1]. All India Reporter
[2]. Judgment Today
[3]. Supreme Court Cases
[4]. Supreme Court Journal

[5]. Supreme Court Weekly

F. Magazines

[1]. Competition Success Review
[2]. Competition Wizard
[3]. Frontline
[4]. India Today
[5]. Kurukchetra
[6]. The Nation and the World
[7]. Outlook
[8]. Pratiyogita Darpan
[9]. The Week
[10]. Yojana

G. Newspapers

[1]. Amar Ujala
[2]. Dainik Jagaran
[3]. The Economic Times
[4]. The Hindu
[5]. Hindustan
[6]. The Hindustan Times
[7]. The Indian Express
[8]. The Pioneer
[9]. Rashtriya Sahara
[10]. The Statesman
[11]. The Times of India

H. Dictionaries and Encyclopedia

[1]. Black's Dictionary of Law, Fifth Edition.
[2]. Mitra's Legal and Commercial Dictionary (New Delhi, Eastern Law House, 5th ed. 1995).
[3]. Oxford Advanced Learner's Dictionary (Oxford University Press, New Delhi, India, 7th ed. 2010).
[4]. P. Ramanath Aiyar: Concise Law Dictionary (Wadhwa and Wadhwa Company, Nagpur, 8th ed. 2008).

[5]. Encyclopedia Britannica Online Academic Edition., *available at*: *http://*www.britannica.com/EBchecked/topic/183748/e-commerce (last visited on February 1, 2014).

[6]. Wehmeier, Sally (eds.), *Oxford Advanced Learner's Dictionary of Current English* (Oxford University Press, 7th edn., 2005).

[7]. Black's Law Dictionary

[8]. Chamber 21 Century Dictionary

[9]. Osborn's S Concise Law Dictionary

[10]. P. Ramanatha Aiyar Concise Law Dictionary

[11]. The Concise Oxford Dictionary

[12]. Webster Third New International Dictionary

I. Websites

[1]. *http://*www.accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html

[2]. *http://*www.articlesbase.com/cyber-law-articles/econtracts-in-cyber-space-502731.html

[3]. *http://*www.ashishlal.wordpress.com/2011/02/12/online-contract-in-context-of-internet/

[4]. *http://*www.asianlaws. orglibrarycyber-lawselectronic-contracts.pdf

[5]. *http://*www.bfvlaw.comwp-contentuploads201210piercy_georgia-electronic-transactions.pdf

[6]. *http://*www.bileta.ac.uk /02papers/basu.html

[7]. *http://*www.biodiv.org

[8]. *http://*www.cato.org/pubs/books/mpney

[9]. *http://*www.comlinkeddocsueta.pdf

[10]. *http://*www.commerce.nic.in /trade/international_trade_oi_ecommerce.asp

[11]. *http://*www.cyberspacelaw .com/ crimes.asp

[12]. *http://*www.digital.law.washington.edu/dspace-law/handle/1773.1/1199

[13]. *http://*www.digitalcommons.law.uga.edu/cgi/viewcontent. gi?article=1023...stu...

[14]. *http://*www.download.Springer.Comstaticpdf186art%253a 10.1007%252fs10660-010-9046-0.Pdfauth66=1393853765_Ceb2a84f1fc05f57feba8b3b56086344 &Ext=.Pd

[15]. *http://*www.*dqindia.ciol.com/content/top_stories/2010/1010122701.asp*accessindia.org.in/pipermail/accessindia_accessindia.org.in/2009-July/028297.html

[16]. *http://*www.ecommercetimes.comlperllstory/4020.html.

[17]. *http://*www.ehealthstrategies.comfiles_primer.pdf

[18]. *http://*www.eldis.org/go/topics/resource-guides/food-security

[19]. *http://*www.enitac.fr/cerpat

[20]. *http://*www.ethno-terroirs.cnrs.fr

[21]. *http://*www.europa.eu.int.

[22]. *http://*www.european-patent-o_ce.org

[23]. *http://*www.ex.ac.ukRDavies /arian/emoneyfaq.html

[24]. *http://*www.expertscolumn.com/content/electronic-contracts-understandingdigital-goods-their-sale-and-purchase

[25]. *http://*www.fao.org

[26]. *http://*www.fao.org/ag/cgrfa/itpgr.htm

[27]. *http://*www.fibre2fashion.comindustry-articlemarket-research-industry-reportsemerging-trend-of-e-commerce-in-indiaemerging-trend-of-e-commerce-in-india1.asp

[28]. *http://*www.gartner.com.

[29]. *http://*www.genecampaign.org

[30]. *http://*www.gis-syal.agropolis.fr

[31]. *http://*www.grain.org

[32]. *http://*www.greenpeace.org/india

[33]. *http://*www.greenpeace.org/international

[34]. *http://*www.huis.hiroshima-u.ac.jp/Computer/Jargon/LexiconEntries/Logic_bomb.html.

[35]. *http://*www.icar.org.in/faqs/ipr.htm

[36]. *http://*www.icrier.orgpdfwp-86.pdf

[37]. *http://*www.ictsd.org

[38]. *http://*www.internationallawoffice.comnewslettersdetail.aspxg=cb904b3a-bda1-491e-a880-19c85da5b1fe#applicable

[39]. *http://*www.iprcommission.org

[40]. *http://*www.iprsonline.org

[41]. *http://*www.ip-watch.org

[42]. *http://*www.irfd.org/events/wf2003/ papers_global /R38.pdf

[43]. *http://*www.isoc.org/inet99/proceedings/3g/3g_2.htm

[44]. *http://*www.jmls.cdu/cyber/statutcs/udsa.html.

[45]. *http://*www.jurisonline.in

[46]. *http://*www.kalpavriksh.org

[47]. *http://*www.kantei.go.jp/foreign/980817densi.html

[48]. *http://*www.knownetgrin.honeybee.org/knownetgrin.html

[49]. *http://*www.legalserviceindia.com/article/l127-E-Contracts.html

[50]. *http://*www.lexvidhi.com/article-details/electronic-contracts-a-basic-

[51]. *http://*www.llrx.com/features/eu_ecom.htm

[52]. *http://*www.mondaq.comindiax22619income+taxdefining+jurisdictions+in+ecommerce+ taxations

[53]. *http://*www.nalsarpro.org /CL/Modules/Module%201/Chapter3.pdf

[54]. *http://*www.narasappa.com/resources/e-ContractsbyAshwini Vittalachar.pdf

[55]. *http://*www.nbaindia.org

[56]. *http://*www.nishithdesai.comfileadminuser_uploadpdfsElectronic_Commerce_Taxation_ evolves_in_India.pdf

[57]. *http://*www.nishithdesai.comResearch-PapersLegal_issues_ecom.pdf

[58]. *http://*www.nopatents-on-seeds.org

[59]. *http://*www.*oecd. org/sti/2093249.pdf*

[60]. *http://*www.origin-food.org

[61]. *http://*www.origin-gi.com

[62]. *http://*www.pcworld.comlnewsarticle. asp?aid= 17868.

[63]. *http://*www.prodottitipici.com

[64]. *http://*www.rimisp.org/territorioeidentidad2

[65]. *http://*www.rimtengg.comiscetproceedingspdfsadv_ nw_tech43 .pdf

[66]. *http://*www.scl.org. /content/commerce

[67]. *http://*www.siliconvalley.com/mldlsiliconvalley/news/editoriaI /S1S6629.htm

[68]. *http://*www.sitesremarquablesdugout.com

[69]. *http://*www. ssrn.com/abstract=1009945

[70]. *http://*www.ssrn.com/abastract=994574

[71]. *http://*www.terroirsetcultures.org

[72]. *http://*www.tkdl.res.in

[73]. *http://*www.twnside.org.sg/access.htm

[74]. *http://*www.uncitral.org/cn-index.htm.

[75]. *http://*www.unctad.orgenDocsposdtem11.en.pdft

[76]. *http://*www.unescap. orgtidpublicationpart_three2261_ind.pdf

[77]. *http://*www.unidroit. orgenglishpublications reviewarticles2000-4-gabriel-e.pdf

[78]. *http://*www.uop.edu.jodownloadresearchmembersWIPO.pdf

[79]. *http://*www.upov.int

[80]. *http://*www.wdwlaw.ca/electronic_contracts_111007_2803 12. pdf

[81]. *http://*www.wipo.int

[82]. *http://*www.wipo.intexportsiteswwwsmeene_commercepdfip_ecommerce.pdf

[83]. *http://*www.wto.org